

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Koichiro AKIYAMA

GAU:

SERIAL NO: New Application

EXAMINER:

FILED: Herewith

FOR: BROADCAST RECEIVING METHOD AND APPARATUS AND INFORMATION DISTRIBUTING
METHOD AND APPARATUS

REQUEST FOR PRIORITY

ASSISTANT COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date of U.S. Provisional Application Serial Number, filed, is claimed pursuant to the provisions of 35 U.S.C. §119(e).
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2000-199629	June 30, 2000

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number .
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
(B) Application Serial No.(s)
- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Marvin J. Spivak

Registration No. 24,913

C. Irvin McClelland
Registration Number 21,124



22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 10/98)

#2
mm
12601

J1036 U.S. PTO
09/893667



日 本 国 特 許 庁
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年 6月30日

出 願 番 号

Application Number:

特願2000-199629

出 願 人

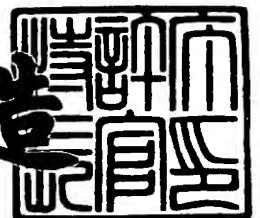
Applicant(s):

株式会社東芝

2001年 5月11日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3039533

【書類名】 特許願

【整理番号】 A000003825

【提出日】 平成12年 6月30日

【あて先】 特許庁長官 殿

【国際特許分類】 H04H 1/00

【発明の名称】 放送受信方法および放送受信装置および情報配信方法および情報配信装置

【請求項の数】 20

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

【氏名】 秋山 浩一郎

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 放送受信方法および放送受信装置および情報配信方法および情報配信装置

【特許請求の範囲】

【請求項 1】 放送配信された暗号化されたコンテンツ情報を受信する複数の受信装置のそれぞれが、各受信装置で復号可能なコンテンツ情報の選択を行うために必要な各受信装置に固有の情報を含む制御情報を用いて、復号すべきコンテンツ情報の選択および復号を行うための放送受信方法において、

前記受信装置は前記制御情報を記憶手段に記憶し、この制御情報の一部または全部を更新するための前記受信装置毎の個別制御情報を双方向通信により受信して、前記記憶された制御情報を更新するとともに、放送配信された前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報を受信し、この鍵情報と前記制御情報とを基に前記放送配信されたコンテンツ情報の選択および復号を行うことを特徴とする放送受信方法。

【請求項 2】 放送配信された暗号化されたコンテンツ情報を受信する複数の受信装置のそれぞれが、各受信装置で復号可能なコンテンツ情報を復号するために必要な各受信装置に固有の情報を含む復号制御情報を用いて、復号すべきコンテンツ情報の復号を行うための放送受信方法において、

前記受信装置は前記復号制御情報を記憶手段に記憶し、この復号制御情報の一部または全部を更新するための前記受信装置毎の個別制御情報を双方向通信により受信して、前記記憶された復号制御情報を更新するとともに、放送配信された前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報を受信し、この鍵情報と前記復号制御情報とを基に前記放送配信されたコンテンツ情報を復号することを特徴とする放送受信方法。

【請求項 3】 放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の選択および復号を行う放送受信装置において、

前記放送配信されたコンテンツ情報の選択のために必要な自装置に固有の情報を含む制御情報を記憶する記憶手段と、

この記憶手段に記憶された制御情報の一部または全部を更新するための個別制

御情報を配信する第 1 の配信装置との間の双方向通信によって、自装置宛の個別制御情報を受信する第 1 の受信手段と、

この第 1 の受信手段で受信された個別制御情報に基づき前記記憶手段に記憶された制御情報を更新する更新手段と、

前記コンテンツ情報を復号するために必要な全ての前記放送受信装置に共通の鍵情報を配信する第 2 の配信装置から放送配信された前記鍵情報を受信する第 2 の受信手段と、

前記記憶手段に記憶された制御情報と前記第 2 の受信手段で受信された鍵情報とを基に前記放送配信されたコンテンツ情報の選択および復号を行うことを特徴とする放送受信装置。

【請求項 4】 放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報を復号する放送受信装置において、

前記放送配信されたコンテンツ情報の復号のために必要な自装置に固有の情報を含む復号制御情報を記憶する記憶手段と、

この記憶手段に記憶された復号制御情報の一部または全部を更新するための個別制御情報を配信する第 1 の配信装置との間の双方向通信によって、自装置宛の個別制御情報を受信する第 1 の受信手段と、

この第 1 の受信手段で受信された個別制御情報に基づき前記記憶手段に記憶された復号制御情報を更新する更新手段と、

前記コンテンツ情報を復号するために必要な全ての前記放送受信装置に共通の鍵情報を配信する第 2 の配信装置から放送配信された前記鍵情報を受信する第 2 の受信手段と、

前記記憶手段に記憶された制御情報と前記第 2 の受信手段で受信された鍵情報とを基に前記放送配信されたコンテンツ情報を復号することを特徴とする放送受信装置。

【請求項 5】 前記個別制御情報は、自装置に固有の鍵情報で復号可能なように暗号化されていることを特徴とする請求項 3 または 4 記載の放送受信装置。

【請求項 6】 前記鍵情報は、前記個別制御情報に含まれる他の鍵情報で復号可能なように暗号化されていることを特徴とする請求項 3 または 4 記載の放送

受信装置。

【請求項 7】 前記鍵情報は、別途受信した鍵生成情報に基づき生成される他の鍵情報で復号可能なように暗号化されていることを特徴とする請求項 3 または 4 記載の放送受信装置。

【請求項 8】 前記個別制御情報は、前記第 1 の配信装置から認証された後受信することを特徴とする請求項 3 または 4 記載の放送受信装置。

【請求項 9】 前記コンテンツ情報の利用に対する課金に必要な利用履歴を前記第 1 の配信装置に送信した後、前記個別制御情報を受信することを特徴とする請求項 3 または 4 記載の放送受信装置。

【請求項 10】 前記個別制御情報の受領を前記第 1 の配信装置へ送信する請求項 3 または 4 記載の放送受信装置。

【請求項 11】 放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う受信装置に記憶されている前記コンテンツ情報の復号のために必要な該受信装置に固有の情報を含む復号制御情報の一部または全部を更新するための個別制御情報を前記受信装置と双方向通信を行って配信することを特徴とする情報配信方法。

【請求項 12】 放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う受信装置であって前記コンテンツ情報の復号を行うために必要な前記受信装置に固有の情報を含む復号制御情報と前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報とを基に前記放送配信されたコンテンツ情報の復号を行う受信装置に対し、前記鍵情報を放送配信することを特徴とする情報配信方法。

【請求項 13】 放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う受信装置に記憶されている前記コンテンツ情報の復号のために必要な該受信装置に固有の情報を含む復号制御情報の一部または全部を更新するための個別制御情報を前記受信装置と双方向通信を行って配信する配信手段を具備したことを特徴とする情報配信装置。

【請求項 14】 放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う受信装置であって前記コンテンツ情報の

復号を行うために必要な前記受信装置に固有の情報を含む復号制御情報と前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報とを基に前記放送配信されたコンテンツ情報の復号を行う受信装置に対し、前記鍵情報を放送配信する配信手段を具備したことを特徴とする情報配信装置。

【請求項 1 5】 前記個別制御情報は、前記受信装置に固有の鍵情報で復号可能なように暗号化して配信することを特徴とする請求項 1 3 記載の情報配信装置。

【請求項 1 6】 前記鍵情報は、別途配信する前記復号制御情報の一部または全部を更新するための個別制御情報に含まれる他の鍵情報で復号可能なように暗号化して配信することを特徴とする請求項 1 4 記載の情報配信装置。

【請求項 1 7】 前記鍵情報は、別途配信する鍵生成情報に基づき生成される他の鍵情報で復号可能なように暗号化して配信することを特徴とする請求項 1 4 記載の情報配信装置。

【請求項 1 8】 前記個別制御情報は、前記受信装置を認証してから配信することを特徴とする請求項 1 3 記載の情報配信装置。

【請求項 1 9】 前記コンテンツ情報の利用に対する課金に必要な利用履歴を前記受信装置から受信した後、前記個別制御情報を配信することを特徴する請求項 1 3 記載の情報配信装置。

【請求項 2 0】 前記個別制御情報の受領を前記受信装置から受信して前記受信装置の復号制御情報が更新されたことを確認する確認手段をさらに具備したことを特徴とする請求項 1 3 記載の情報配信装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、例えば、有料放送システムに関する。

【0 0 0 2】

【従来の技術】

デジタル放送は、通信衛星（C S）に始まって、ケーブル T V、地上放送へとデジタル化が進むにつれ、一層のサービスの充実が期待されており、これからに

放送サービスの主役をつとめていくものと思われる。

【 0 0 0 3 】

デジタル放送の最大の特徴は、情報圧縮技術の導入により、番組の送信に要する周波数の使用効率の向上が図れ、アナログ放送に比較して放送チャンネル数の大幅な増加が可能になってことである。更に、高度な誤り訂正技術が適用できるため、高品質で均質なサービスの提供が可能となる。

【 0 0 0 4 】

また、デジタル化により従来のように画像や音声による放送だけでなく、文字やデータによる放送（データ放送）も可能になり、例えばニュースを文字データとして流すことや、PCソフトを放送で配信することが可能となり、そのようなサービスを提供するためのシステムも続々登場してきている。また、受信装置も従来のような据え置き型だけでなく、移動中でも利用できる携帯情報端末、自動車の中での利用を前提とし、自動車に据え付けられている移動端末などモバイル型受信装置も出現している。

【 0 0 0 5 】

このようなシステムにおいて有料放送サービスを実現する際には、放送コンテンツを暗号化して送信し、契約内容に基づいてスクランブルを解くなど、契約期間、契約内容に即した顧客管理が行えなければいけない。契約期間に即した顧客管理とは、例えば、所定の料金の支払により契約された契約期間内に限って契約チャンネルに番組を可能とするというものである。

【 0 0 0 6 】

また、受信装置にてスクランブルあるいは暗号を解くための鍵情報は、不正視聴を防止する上からも正当な視聴者のみに（契約チャンネル、契約期間に即して）しかも確実に提供する必要がある。

【 0 0 0 7 】

これを実現するため、従来は放送受信装置毎にマスター鍵を用意し、受信契約している視聴者に対して受信契約しているチャンネルのワーク鍵と視聴可能なチャンネル情報などを含む契約形態を示した契約情報をマスター鍵で暗号化して放送波で送信していた。ここでワーク鍵はチャンネル固有の鍵であり、暗号化されて送ら

れてくる当該チャネルのチャネルキーを復号することができる。チャネルキーはスクランブル(暗号化)された放送コンテンツをデスクランブル(復号)するのに用いられる。

【0008】

このような限定受信方式では(受信装置毎に設定された)マスター鍵で暗号化されるワーク鍵と契約情報は受信装置固有の限定受信情報であり、(複数の受信装置に共通の)ワーク鍵で暗号化されたチャネルキーは共通の限定受信情報であると言える。

【0009】

【発明が解決しようとする課題】

従来は、固有の限定受信情報であっても(固有情報を送信するには不適當な)放送波によって送信していた。これは、個別の加入者に対する情報を全ての加入者に送信しているため不必要に送信帯域を専有しているばかりか、加入者が受信したかどうかの情報も得ることができないため、必要な期間繰り返し送信する必要があった。

【0010】

更に、個別の限定受信情報に含まれるワーク鍵は契約期間(通常1ヶ月)毎に設定され、その期間毎に放送局から個別に限定受信情報を送らなくてはならない上に、受信装置が実際に受信したか否かが契約管理センター側に分からないため、一定期間繰り返し送信しなければならなかった。このため現在限定受信情報に占める個別の限定受信情報の割合が相当に大きくなっている。

【0011】

一方、現在CS放送などでは視聴する番組に対して課金するPPV(ペイパービュー)サービスが行われているが、加入者が視聴操作後すぐに視聴できるよう便宜を図るため、視聴操作の際に直接契約管理センターに連絡することはせず、受信装置本体内に受信履歴を格納しておいて、センターは定期的に当該受信履歴を回収するようにしている。しかし、このように構成しているため加入者が故意または偶然にセンターが受信履歴を回収するため接続している公衆電話回線を外すなどの操作を行ってしまった場合は回収ができなくなるという問題もあった。

【 0 0 1 2 】

そこで、本発明は、このような現状に鑑み、加入者が増加しても放送帯域を圧迫することなく、不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする放送受信方法およびそれを用いた放送受信装置および情報配信方法およびそれを用いた情報配信装置を提供することを目的とする。

【 0 0 1 3 】

更に、PPVサービスに必須の視聴履歴の回収が容易に行え、視聴料も安全かつ確実に回収できる放送受信装置および情報配信装置を提供することを目的とする。

【 0 0 1 4 】

【課題を解決するための手段】

本発明は、放送配信された暗号化されたコンテンツ情報を受信する複数の受信装置のそれぞれが、各受信装置で復号可能なコンテンツ情報の選択を行うために必要な各受信装置に固有の情報を含む制御情報（例えば、チャンネル契約情報、ワーク鍵）を用いて、復号すべきコンテンツ情報の選択および復号を行うためのものであって、前記受信装置は前記制御情報を記憶手段に記憶し、この制御情報の一部または全部（例えば、チャンネル契約情報＋ワーク鍵、チャンネル契約情報のみ、ワーク鍵のみ）を更新するための前記受信装置毎の個別制御情報を双方向通信により受信して、前記記憶された制御情報を更新するとともに、放送配信された前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報（例えば、チャンネルキー）を受信し、この鍵情報と前記制御情報とを基に前記放送配信されたコンテンツ情報の選択および復号を行うことを特徴とする。

【 0 0 1 5 】

本発明は、放送配信された暗号化されたコンテンツ情報を受信する複数の受信装置のそれぞれが、各受信装置で復号可能なコンテンツ情報を復号するために必要な各受信装置に固有の情報を含む復号制御情報（例えば、チャンネル契約情報＋ワーク鍵＋マスター鍵、チャンネル契約情報＋マスター鍵、ワーク鍵＋マスター鍵）を用いて、復号すべきコンテンツ情報の復号を行うためのものであって、前記受信装置は前記復号制御情報を記憶手段に記憶し、この復号制御情報の一部また

は全部（例えば、チャンネル契約情報＋ワーク鍵、チャンネル契約情報のみ、ワーク鍵のみ）を更新するための前記受信装置毎の個別制御情報を双方向通信により受信して、前記記憶された復号制御情報を更新するとともに、放送配信された前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報（例えば、チャンネルキー）を受信し、この鍵情報と前記復号制御情報とを基に前記放送配信されたコンテンツ情報を復号することを特徴とする。

【 0 0 1 6 】

好ましくは、前記個別制御情報は、各受信装置に固有の鍵情報で復号可能なように暗号化されている。また、好ましくは、前記鍵情報は、前記個別制御情報に含まれる他の鍵情報で復号可能なように暗号化されている。また、好ましくは、前記鍵情報は、別途受信した鍵生成情報に基づき生成される他の鍵情報で復号可能なように暗号化されている。また、好ましくは、前記個別制御情報は、通信相手から認証された後受信する。また、好ましくは、前記個別制御情報の受領を通信相手へ送信する。

【 0 0 1 7 】

本発明によれば、各受信装置は、全ての受信装置に共通の鍵情報を放送にて、各受信装置個別の個別制御情報を電話回線等の双方向通信によって取得するので、加入者が増加しても大量の個別制御情報を配信することにより放送帯域を圧迫することなく、さらに不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする。

【 0 0 1 8 】

また、前記コンテンツ情報の利用に対する課金に必要な利用履歴を通信相手へ送信した後、前記個別制御情報を受信することにより、PPVサービスに必須の視聴履歴の回収が容易に行え、視聴料も安全かつ確実に回収できる。

【 0 0 1 9 】

本発明は、放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う受信装置に記憶されている前記コンテンツ情報の復号を行うために必要な情報を含む該受信装置に固有の復号制御情報の一部または全部を更新するための個別制御情報を前記受信装置と双方向通信を行って配信

することを特徴とする。好ましくは、前記個別制御情報は、前記受信装置に固有の鍵情報で復号可能なように暗号化して配信する。また、好ましくは、前記個別制御情報は、前記受信装置を認証してから配信する。また、好ましくは、前記個別制御情報の受領を前記受信装置から受信して前記受信装置の復号制御情報が更新されたことを確認する。

【 0 0 2 0 】

本発明によれば、各受信装置は、全ての受信装置に共通の鍵情報を放送にて、各受信装置個別の個別制御情報を電話回線等の双方向通信によって取得するので、加入者が増加しても大量の個別制御情報を配信することにより放送帯域を圧迫することなく、さらに不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする。

【 0 0 2 1 】

また、前記コンテンツ情報の利用に対する課金に必要な利用履歴を前記受信装置から受信した後、前記個別制御情報を配信することにより、P P Vサービスに必須の視聴履歴の回収が容易に行え、視聴料も安全かつ確実に回収できる。

【 0 0 2 2 】

本発明は、放送配信された暗号化されたコンテンツ情報を受信して、復号可能なコンテンツ情報の復号を行う受信装置であって、前記コンテンツ情報の復号を行うために必要な前記受信装置に固有の情報を含む復号制御情報と前記受信装置に依存しない前記コンテンツ情報を復号するために必要な鍵情報とを基に前記放送配信されたコンテンツ情報を復号する受信装置に対し、前記鍵情報を放送配信することを特徴とする。好ましくは、前記鍵情報を、別途配信する前記復号制御情報の一部または全部を更新するための個別制御情報に含まれる他の鍵情報で復号可能なように暗号化して配信する。また、好ましくは、前記鍵情報は、別途配信する鍵生成情報に基づき生成される他の鍵情報で復号可能なように暗号化して配信する。

【 0 0 2 3 】

本発明によれば、前記放送受信装置に対し、不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする。

【 0 0 2 4 】

【発明の実施の形態】

本発明の実施形態について図面を参照して説明する。

【 0 0 2 5 】

まず、用語の定義を行う。1つまたは複数のチャンネルからなる放送コンテンツの受信に際し、暗号化などを施して所定の契約・加入手続きなどを行った限られた者（以下、正規の契約者あるいは加入者あるいはユーザと呼ぶ）だけに放送コンテンツの視聴を許可することを総称して限定受信という。また、限定受信を実現するシステムを総称して限定受信システムという。本実施形態では、例えば、有料放送サービスのための限定受信システムを例にとり説明する。

【 0 0 2 6 】

限定受信を行なうため各加入者毎にチャンネル毎の契約状態を記述した情報をチャンネル契約情報と呼ぶ。例えば各チャンネルにチャンネル番号を付け、図2のようにチャンネル番号に対応したビットが「1」であるか否かによりチャンネルの契約状態を表したビット列がチャンネル契約情報である。図2では第2、第5、第7、第8チャンネルが契約されていることを示している。

【 0 0 2 7 】

更に、図6に示すように、図2に示したチャンネル契約情報に当該チャンネル契約情報の有効期限などチャンネル契約情報に制限を加える情報や、加入者の契約形態をより詳細に表現する情報を付加してチャンネル契約情報が構成されていてもよい。

【 0 0 2 8 】

本実施形態に係る有料放送サービスの各加入者は、それぞれ契約内容（視聴したいチャンネルや視聴する期間など）が異なる。すなわち、これら加入者の所持する放送受信装置への限定受信を可能にするためには、各加入者毎に異なる契約内容（利用条件）に基づく当該放送受信装置の制御情報を個別に配信する必要がある。このような制御情報を個別制御情報と呼ぶ。なお、個別制御情報は、パケット形式で配信されるため、その場合は、個別制御パケットとも呼ぶ。この個別制御パケットは、例えば、現行CS放送規格におけるEMM（Entitlement Manag

ement Message)、 EMM-S (Entitlement Management Message for S-band) に当たる (参考文献「BSデジタル放送限定受信方式 標準規格 ARIB STD-B25 (電波産業会))」。

【 0 0 2 9 】

放送コンテンツ情報 (以下、簡単にコンテンツと呼ぶことがある) は、各チャンネル毎に異なった鍵情報、すなわち、ここでは「チャンネルキー」で暗号化されている。よって、各加入者の所持する放送受信装置にて所望の (契約した) チャンネルのコンテンツを視聴するためには、このコンテンツ情報に依存する鍵情報のような全ての加入者 (加入者の所持する全ての放送受信装置) に共通の制御情報も配信する必要がある。このような制御情報を共通制御情報と呼ぶ。なお、共通制御情報も、パケット形式で配信されるため、その場合は、共通制御パケットとも呼ぶ。この共通制御パケットは、例えば、現行CS放送規格におけるECM (Entitlement Control Message)、ECM-S (Entitlement Control Message for S-band) に当たる (参考文献「BSデジタル放送限定受信方式 標準規格 ARIB STD-B25 (電波産業会))。

【 0 0 3 0 】

各加入者の所持する放送受信装置は、個別制御情報と共通制御情報とを確実に受信することにより、各加入者の契約内容に沿ったコンテンツ情報の視聴が可能になるわけである。

【 0 0 3 1 】

以下の実施形態を通じて、受信装置内部で限定受信方法を実現する構成 (主にハードウェア) を限定受信部あるいは限定受信チップという。限定受信チップには限定受信のための秘密情報が含まれているので内部のメモリやハード構成に関して外部から容易に読み出し、書き込み、変更ができない耐タンパ構造を仮定している。

【 0 0 3 2 】

なお、以下の説明において、暗号化されたコンテンツ情報をチャンネルキーを用いて復号することをデスクランブルと呼ぶこともある。

【 0 0 3 3 】

さらに、以下の実施形態で説明する限定受信システムは、主に、サービス加入者の所持する放送受信装置と、この放送受信装置に個別制御情報、共通制御情報、暗号化コンテンツ情報等を配信する契約管理センター（以下、簡単にセンターと呼ぶことがある）としての情報配信装置（契約管理装置とも呼ぶ）とから構成される。

【 0 0 3 4 】

以下の実施形態において、例えば、双方向通信に係る機能とは、送受信部 1 0 2、モデム部 1 0 1 に対応するが、本発明は、限定受信部に特徴があるので、双方向通信機能部の詳細構成とその説明は省略する。例えば、送受信部 1 0 2 に所定の接続ケーブルを用いてを接続して双方向通信機能部を構成することもできる。

【 0 0 3 5 】

（第 1 の実施形態）

以下、本発明の第 1 の実施形態について説明する。

【 0 0 3 6 】

第 1 の実施形態は、各受信装置が個別のマスター鍵を有する場合の限定受信システムである。このような限定受信システムは各受信装置に対し、定期的にしかも個別にチャンネル契約情報等を含む制御情報を暗号化して送信しなければならないので限定受信の送信量が大きくなるという問題点がある。だがその反面マスター鍵が破られた際の被害範囲が狭いなど、安全性が高いため従来から C S 放送その他で採用されてきた。しかし、近年の加入者の増加に伴って、受信装置個別に送付すべき制御情報の量が膨大になってきており、本実施形態はこの解決策を与えるものである。

【 0 0 3 7 】

このような限定受信システムでは、例えば、図 3 に示すような鍵構成を採用している。即ちチャンネル毎に定められている全ての受信装置に共通のワーク鍵 K_w を個別のマスター鍵 K_M で暗号化して送信する。更に、そのワーク鍵 K_w を使ってチャンネルキー K_{ch} を暗号化して送信する。放送コンテンツはチャンネルキー K_{ch} を使って慣用暗号方式で暗号化されているので、このチャンネルキーで復号で

きる。ここでチャネルキーは解読を防ぐため通常10分程度の短時間で変更しなくてはならない。これを送信するために個別のマスター鍵を使っていたのでは送信量が膨大となる。そのため全受信装置に共通のワーク鍵を使う必要がある。またワーク鍵も何ヵ月という単位で同じ鍵を使うと危険なので、変更する必要がある。これを個別のマスター鍵で暗号化する仕組みとなっている。このことにより、例えマスター鍵が知られても、ワーク鍵を変更することによって無料視聴を防止することができる。

【0038】

さて、本実施形態の限定受信システムにおいて放送受信装置が放送波を介して受信するデータはコンテンツパケット、共通制御パケットの2種類である。コンテンツパケットは図4に示すパケット形式で、情報識別子、チャネル識別子、チャネルキー識別子、スクランブルされた（チャネルキーで暗号化された）放送コンテンツからなっている。

【0039】

情報識別子は当該パケットの種別を示すもので、ここではコンテンツパケットであることを示す識別子を記述する。チャネル識別子は当該放送コンテンツがどのチャネルのコンテンツかを示すものである。また、チャネルキー識別子は当該放送コンテンツを復号するチャネルキーの識別子を示す。放送コンテンツは生の番組データで、チャネルキー識別子で指定されたチャネルキー K c h で暗号化されている。尚、本実施形態ではこれら全ての情報は固定長で表現されたデータであるとする。

【0040】

共通制御パケットは、図8に示すパケット形式で、情報識別子、ワーク鍵識別子、チャネル識別子、チャネルキー識別子（1）、チャネルキー（1）、チャネルキー識別子（2）、チャネルキー（2）で構成されており、チャネル識別子からチャネルキー（2）までの部分はワーク鍵識別子で示されたワーク鍵で暗号化されている。

【0041】

情報識別子は当該パケットの種別を示すもので、ここでは共通制御パケットで

あることを示す識別子を記述する。チャンネル識別子は当該共通制御パケットがどのチャンネルのものを示すものである。また、ワーク鍵識別子は当該共通制御パケットがどのワーク鍵 K_w によって暗号化されているかを示す情報である。チャンネルキー識別子は次に記述されているチャンネルキーの識別子であり、チャンネルキーはチャンネル識別子で指定されているチャンネルの放送コンテンツの暗号化に使われているチャンネルキーを示している。

【 0 0 4 2 】

ここで、チャンネルキー識別子とチャンネルキーが2組存在するのは、前記のようにチャンネルキーは比較的短時間で変更されるため、チャンネルキーの切り替えをスムーズに行う必要から現在使っているチャンネルキーと次回使うチャンネルキーを同時に送っているからである。もちろん、このように2組送信することは本発明には直接影響しないので、1組であっても構わない。

【 0 0 4 3 】

本実施形態に係る放送受信装置は、個別制御情報を公衆電話回線からモデムを経由して受信する。個別制御情報も共通制御情報と同様にパケット形式で送信される。個別制御パケットは図7に示すように情報識別子、マスター鍵識別子、暗号化された契約情報からなっている。情報識別子は当該パケットの種別を示すもので、ここでは個別制御パケットであることを示す識別子を記述する。マスター鍵識別子は暗号化された契約情報を復号可能なマスター鍵の識別情報であり、正しく送受信されていれば、ここには当該パケットを受信した受信装置の有するマスター鍵識別子が記述されている。

【 0 0 4 4 】

契約情報とは、例えば、図5に示すように、受信装置ID、チャンネル契約情報、ワーク鍵の数 n 及び n 個のワーク鍵とワーク鍵識別子のペア、デジタル署名からなっている。受信装置IDは当該契約情報を受信すべき受信装置の識別子であり、正常の送受信されていれば受信装置内部の限定受信部内にある受信装置IDと一致したIDが入る。チャンネル契約情報は当該受信装置IDを有する受信装置の契約状態を示すもので、例えば、図2に示した構成のデータである。ワーク鍵識別子 i は続くワーク鍵 i の識別子である。本実施形態においてワーク鍵はチ

チャンネル毎に設定されているため、チャンネル契約情報に対応したワーク鍵とワーク鍵識別子の組が入る。デジタル署名は当該契約情報の正当性を確認するための情報であり、主に偽造防止のために用いる。尚、本実施形態ではこれら全ての情報は固定長で表現されたデータであるので、受信されたパケットから各情報を抽出するアルゴリズムは改めて述べない。

【 0 0 4 5 】

次に、本実施形態の放送受信装置（簡単に受信装置と呼ぶことがある）の構成と処理動作について説明する。放送受信装置の要部の構成図を図 1 に、双方向通信にて（例えば公衆網経由で）配信される情報（個別制御パケット）の受信処理動作を図 9 に、放送波で配信される情報（共有制御パケットとコンテンツパケット）の受信処理動作を図 1 0 ～図 1 3 に示す。

【 0 0 4 6 】

まず、公衆回線経由で受信される個別制御パケットの受信処理動作を図 1 を参照しながら図 9 に基づいて説明する。図 1 の放送受信装置は個別制御パケットを受信する際、まず、限定受信管理センターからの発呼に対し、当該受信装置が応答することによって個別制御パケットを送受信するためセッションが確立される（ステップ S 1）。

【 0 0 4 7 】

受信装置の個別制御情報受信部 1 0 2 は、公衆網、モデム部 1 0 1 を介して個別制御パケットを受信すると（ステップ S 2）、その情報識別子からそのパケットが個別制御パケットであることを認識し、当該パケットからマスター鍵識別子を取得する。個別制御情報受信部 1 0 2 は、取得したマスター鍵識別子がマスター鍵格納部 1 0 3 に格納されているマスター鍵に対応したマスター鍵識別子でなければ、当該確立されているセッションを利用して、センターへエラーを送信する（ステップ S 3、ステップ S 1 0）。対応したマスター鍵識別子であれば、当該マスター鍵をマスター鍵格納部 1 0 3 から出力し（ステップ S 4）、個別情報パケット内の契約情報を復号する（ステップ S 5）。復号された契約情報に含まれるワーク鍵情報（ワーク鍵識別子とワーク鍵のペア等）はワーク鍵格納部 1 0 5 に格納される（ステップ S 1 1）。

【0048】

一方、契約情報認証部107では、復号された契約情報に含まれる受信装置IDと受信装置ID格納部106に格納されている受信装置IDと比較し（ステップS6）、一致しなければ、個別制御情報受信部102を介してセンターヘエラーを出力する（ステップS12）。一致していれば、契約情報認証部107は次に、デジタル署名検証鍵格納部108に格納されている鍵情報（秘密鍵あるいは公開鍵）を用いてデジタル署名を検証し（ステップS7）、検証が成功しなければ、個別制御情報受信部102を介してその旨センターヘエラー返信し（ステップS13）、検証が成功すれば、復号された契約情報に含まれるチャネル契約情報を契約情報格納部121に格納し（ステップS8）、個別制御情報受信部102を介してセンターヘ契約情報の更新が正常終了したことを示す受領通知を送信して終了する（ステップS9）。

【0049】

ここで、契約情報認証部107におけるデジタル署名の検証処理について説明する。ここでいうデジタル署名は大きく分けて2つ考えられる。1つは共通鍵暗号を用いたそれであり、センターと受信装置で共通の暗号アルゴリズムと共通の秘密鍵を持ち、図5の契約情報のうちデジタル署名以外の部分を当該秘密鍵でブロック単位で逐次的に暗号化し、最後のブロックをデジタル署名とする方式である。ここで逐次的な暗号化とは前のブロックが現在のブロックの暗号化に影響を与えるような暗号化の方式である。例えば、現在のブロックを秘密鍵で暗号化し、その暗号化結果と前のブロックの暗号化結果の排他的論理和をもって現在のブロックの暗号化結果とすることによって実現できる。この方法を使うと、途中のブロックを改竄した場合でも、（ほとんどの場合）異なるデジタル署名が生成されるので改竄検出になる。

【0050】

また、デジタル署名には、前記手法以外にもハッシュ値と呼ばれる署名したいデータ全体の特徴量を計算して、その値を暗号化する手法が知られている。ハッシュ値はデータ全体から計算され、データが1ビットでも変更されるとハッシュ値は著しく異なるばかりか、同じハッシュ値をもつデータを作成することが困難

であるという特徴がある。このような性質のため、改竄検出が可能となる。尚、ハッシュ値は固定長データでハッシュ関数で作成される。

【 0 0 5 1 】

共通鍵暗号による署名検証は高速に行えるばかりでなく、回路規模が小さくてすむが、センターと同じ情報を受信装置が持つため、ハッキング等に弱いという特徴がある。

【 0 0 5 2 】

もう1つは公開鍵暗号を用いた方法で、秘密鍵で署名したものを公開鍵で検証する。ここで、公開鍵から秘密鍵を導出することが極めて困難なため、受信装置をハッキングして公開鍵を抽出しても、改竄が相当に困難であることが特徴である。極めて安全性の高い方式であるが、低速であるばかりか、回路規模が大きくなるという弱点もある。

【 0 0 5 3 】

このようなデジタル署名の優れた性質により、受信装置は（個別制御パケットに付加されたデジタル署名を通じて、）情報配信装置（契約管理装置ともいう）認証しているとも言える。しかし、本発明で考える問題点を解決するためにはデジタル署名は必須ではない。すなわち、本発明の個別制御パケットにおいてデジタル署名は必須ではなく、個別制御パケットからデジタル署名を除いた構成でも矛盾なく本発明を実施できる。

【 0 0 5 4 】

次に、放送波で配信される共有制御パケットとコンテンツパケットの受信処理動作について、図1を参照しながら図10～図13を基に説明する。

【 0 0 5 5 】

受信装置は放送波を放送受信部111で受信し（ステップS21）、A/D変換部112でアナログ信号からデジタルデータに変換（A/D変換）する（ステップS22）。デジタル化されたパケットデータは誤り検出／訂正部113に送られ誤り検出／訂正が行われた後（ステップS23～ステップS24）、それぞれのパケットの情報識別子を参照して共通制御パケットとコンテンツパケットのどちらかを判別して、判別結果に応じた処理を施す（ステップS25、ステップ

S 26)。

【0056】

ところで、チャンネル選択インタフェース (I/F) 115は、現在視聴中のチャンネル識別子を取得するもので、ここで取得されたチャンネル識別子はチャンネル選択部114とチャンネル情報入力部123へ渡される (図12のステップS51～ステップS53)。

【0057】

コンテンツパケットである場合は、現在視聴中のチャンネル識別子をチャンネル選択インタフェース (I/F) 115を介して得て、チャンネル選択部114で視聴チャンネルのコンテンツパケットのみを選択して限定受信部100のフィルタ一部116に送信する。フィルタ一部116ではこれをデスクランブル部120へ送る (ステップS27～ステップS28)。

【0058】

一方、共通制御パケットである場合はチャンネル選択部114を経て、フィルタ一部116で共通制御情報復号部117へ送られ、復号が開始される (ステップS41)。

【0059】

次に、コンテンツパケットに関する処理を図11のフローチャートに沿って詳しく説明する。コンテンツパケットは、前記処理によってフィルタ一部116からデスクランブル部120へ送られる。デスクランブル部120は、コンテンツパケットからチャンネル識別子とチャンネルキー識別子を取り出し、それをチャンネルキー出力部119に渡すとともに、チャンネルキーの出力を要請する。チャンネルキー出力部119は契約判定部122での当該チャンネルに対する契約判定を基に受信チャンネルのチャンネルキーをチャンネルキー格納部118から抽出する。

【0060】

すなわち、図12に示すように、契約判定部122は、チャンネル情報入力部123から現在視聴されているチャンネルのチャンネル識別子を取得し (ステップS54)、契約情報格納部121にすでに記憶されている図2に示したようなチャンネル契約情報を参照して、取得したチャンネル識別子に対応するビットが「1」であ

れば「許可」、「0」であれば「不許可」の信号をチャンネルキー出力部 1 1 9 に送る（ステップ S 5 5）。チャンネルキー出力部 1 1 9 では、送られてきた判定結果が「許可」であればチャンネルキー格納部 1 1 8 からコンテンツパケットから取り出されたチャンネルキー識別子を持つチャンネルキーをチャンネルキー格納部 1 1 8 から得て、デスクランブル部 1 2 0 へ渡す（ステップ S 5 7）。判定結果が「不許可」であれば、そこで当該コンテンツパケットに関する処理を終了する。

【 0 0 6 1 】

デスクランブル部 1 2 0 は、チャンネルキー出力部 1 1 9 からチャンネルキーを受け取ると、それを用いてコンテンツパケットに含まれる暗号化されたコンテンツ情報を復号して出力する（図 1 1 のステップ S 2 9 ～ステップ S 3 2）。

【 0 0 6 2 】

次に、共通制御パケットに関する処理を図 1 3 に沿って説明する。共通制御パケットはフィルタ部 1 1 6 から共通制御情報復号部 1 1 7 に送られる。ここで、共通制御パケット内の未暗号部に含まれるワーク鍵識別子を基にワーク鍵格納部 1 0 5 からワーク鍵を取得する（ステップ S 4 2）。ここでワーク鍵が取得できなかった場合、処理を終了する（ステップ S 4 3）。ワーク鍵が取得できたら、当該ワーク鍵で共通制御パケット内の暗号化部の情報を復号する（ステップ S 4 4）。復号された情報からチャンネルキー K c h を取得し、チャンネルキー格納部 1 1 8 に格納する（ステップ S 4 5）。

【 0 0 6 3 】

以上説明したように、図 1 に示した放送受信装置によれば、放送受信装置に記憶されて受信したコンテンツ情報の選択および復号に必要なチャンネル契約情報、ワーク鍵を定期的に更新するための個別制御情報を放送波で送信する必要がなくなるばかりか、個別制御情報を受信したか否かが双方向通信による情報の送受信過程でセンター側で把握できるため、繰り返し送信する必要も無くなった。このようなことから、センター側から各加入者へ配信すべき個別制御情報の大幅な削減が可能になった。

【 0 0 6 4 】

（第 2 の実施形態）

次に、上記第1の実施形態のいくつかのバリエーションを述べる。第1のバリエーションは限定受信管理センターから公衆回線を使って個別制御情報を送信する際、個別制御情報を送信する前にチャレンジアドレスポンス型相手認証によって、送信側の受信装置の正当性を確かめるものである。この方式を導入すると、センター側は正当な受信装置しか知り得ない様々なチャレンジ（質問）とそのレスポンス（答え）によって受信装置をより確実に認証することができる。

【 0 0 6 5 】

図14は第1の実施形態の第1のバリエーションに係る放送受信装置の要部の構成例を示したもので、個別制御情報をモデム101経由で取得する際の処理部の構成が図1と異なる。

【 0 0 6 6 】

共通制御情報の受信処理は、前述同様であるので、異なる部分についてのみ説明する。すなわち、個別制御情報の構成とその受信処理動作が異なる。

【 0 0 6 7 】

まず、モデム経由で送受信される個別制御パケットの構成は、図15に示すように、情報識別子と情報本体からなり、この情報本体の違いにより3つのパケットに分類できる。ここでは、例えば、図7に示した個別制御パケットと同様のパケット（以下、このパケットを、他の2種類のパケットを区別するためにあえて個別制御パケットと呼ぶ）とチャレンジパケットとレスポンスパケットとがある。

【 0 0 6 8 】

個別制御パケットの情報本体は、図16に示すように、マスター鍵識別子、暗号化された契約情報からなり、図7と同様であり、契約情報は、図5と同様である。

【 0 0 6 9 】

チャレンジパケットの情報本体は、図17に示すように、チャレンジ番号とチャレンジ情報本体からなっており、チャレンジ番号とはチャレンジと呼ばれるセンターから受信装置への質問や問題の管理番号である。本実施形態で想定しているチャレンジは、受信装置IDを問い合わせるチャレンジ、マスター鍵識別子を

問い合わせるチャレンジ、チャレンジ情報に（受信装置固有の）秘密鍵で署名を作成するチャレンジである。この他にも、暗号化されたチャレンジ情報を秘密鍵で復号させ、復号結果をレスポンスさせるチャレンジもある。ここで秘密鍵で署名させるチャレンジのように対象データが必要な場合、それをチャレンジ情報に記述して送信する。

【 0 0 7 0 】

チャレンジアンドレスポンスの基本は送信先の受信装置とセンターのみしか知り得ない情報を使わないと答えられないように質問をして、その質問に正確に答えられたことで、当該受信装置が（センターの加入者DBに登録されている）正当な装置であることを確認することにある。

【 0 0 7 1 】

レスポンスパケットの情報本体は、図 1 8 に示すように、チャレンジ番号とチャレンジ情報本体、レスポンス情報本体からなっている。レスポンス情報本体も（チャレンジ情報本体と同様に）チャレンジ番号によって形式が定まっているものとする。

【 0 0 7 2 】

以下、図 1 4 を参照しながら、図 1 9 ～図 2 0 に示すフローチャートを参照して個別制御パケットの受信処理動作について説明する。

【 0 0 7 3 】

まず、契約管理センターから各受信装置に対して発呼が行われると（ステップ S 1 0 1）、受信装置がモデム部 1 0 1 を経由してセンター間通信部 1 5 2 でそれを受け、パケットを受信する（ステップ S 1 0 2）。センター間通信解析部 1 5 1 では、受信したパケットをその情報識別子からチャレンジパケットと判別したときは（ステップ S 1 0 3）、それをレスポンス作成部 1 5 2 に送る（ステップ S 1 0 6）。個別制御パケットであったときは（ステップ S 1 0 4）、当該パケットを個別制御情報復号部 1 0 4 へ送信して（ステップ S 1 0 7）第 1 の実施形態と同様の処理によって個別制御情報の認証と格納処理を行う（ステップ S 1 0 8）。受信パケットが上記いずれでもなかった場合はエラーとしてセンターへ送信する（ステップ S 1 0 5）。

【0074】

次に、レスポンスパケットの処理動作について、図20に示すフローチャートを参照して詳しく説明する。

【0075】

チャレンジが受信装置IDの問い合わせであった場合（ステップS111）、レスポンス作成部152は、受信装置ID格納部106から受信装置IDを取り出して（ステップS115）、予め定められたレスポンス情報形式に受信装置IDを変換して、図18に示すようなレスポンスパケットを作成し（ステップS116）、センター間通信部152を介してセンターへ送信する（ステップS117）。

【0076】

チャレンジがマスター鍵識別子の問い合わせであった場合（ステップS112）、マスター鍵識別子を取得して（ステップS118）、前述同様にレスポンスパケットを作成し（ステップS119）、センターへ送信する（ステップS120）。

【0077】

署名作成のチャレンジであった場合は（ステップS113）、署名すべきデータであるチャレンジ情報本体を取得し（ステップS121）、受信装置から秘密鍵格納部153に格納されている秘密鍵を取得して（ステップS122）、チャレンジ情報本体に対する署名を作成する（ステップS123）。作成された署名は予め定められた形式にしたがってレスポンス情報本体の形式に変換され、レスポンスパケットの形式でセンターへ送信される（ステップS123～ステップS125）。上記3通りのどれにも当てはまらない場合は、エラーをセンターに送信する（ステップS114）。

【0078】

センター側では、1つまたは複数のチャレンジを受信装置に送り、受信装置から送られてきたレスポンスが全て正しかったとき、第1の実施形態と同様にして個別制御パケットを送信する。このようにすることによって、送信する受信装置が正当な受信装置であることを確認した上で個別制御情報を送信することができ

るため、不正な改造を施した受信装置を排除することが可能になる。この点が第 1 の実施形態に優る点である。

【 0 0 7 9 】

また、逆に、（第 1 の実施形態でも述べたように）受信装置が情報配信装置（契約管理装置）を認証していると言えるので、本実施形態により受信装置と情報配信装置との間で相互認証が行われていると言える。しかし、第 1 の実施形態でも述べたように、このような形態は本発明において必須でなく、本発明のように情報配信装置（契約管理装置）が受信装置を認証する実施形態が本質的である。

【 0 0 8 0 】

（第 3 の実施形態）

第 2 のバリエーションは、限定受信管理センターから公衆回線を使って個別制御を送信する際、P P V（ペイパービュー）に必須の視聴履歴等の受信装置から回収しなければならない情報を回収するものである。

【 0 0 8 1 】

P P Vとは番組毎の課金を前提とした課金方式である。P P V対象の番組を視聴する場合は加入者自身がリモコン操作などで見たい番組を選択することによって当該番組のスクランブルが解かれ、視聴できるようになる仕組みである。P P Vの視聴料は通常の契約に加算されて請求される仕組みである。現行のP P Vはデスクランブルのための鍵を受信装置側に秘密に保持しており、P P Vの操作があった場合には当該デスクランブル鍵を用いて当該番組をデスクランブルして、受信装置内部のP P V受信履歴格納部に受信履歴を格納するようになっている。

【 0 0 8 2 】

これはP P V受信操作の度にセンターに接続すると、公衆回線が混んだり、通信費がかかったりするなどの障害があるためである。しかしながら現行の方式では受信装置内部のP P V受信履歴を回収する必要がある、（加入者が電話線を外すなどの処置を行った場合は）回収することができなくなるという問題がある。

【 0 0 8 3 】

その点に鑑み本実施形態では契約情報更新とP P V視聴情報回収を同じセッションで行うことにより、一般の契約チャネルを視聴している加入者に対してP P

V視聴情報を定期的に回収できる方式を提案するものである。

【0084】

本実施形態の全体構成図は図21に、主要部分のアルゴリズムを図22、図23に示す。構成的に第1の実施形態及び第2の実施形態として示した第1のバリエーションと重なる部分が多いため、以下ではそれらと異なる部分（PPVに関する部分）のみに関して説明する。

【0085】

センターの発呼を受けて、受信装置がセンターから送信されたパケットを受信し（ステップS201、ステップS202）、受信したパケットがチャレンジパケットであるか、PPV受信履歴回収パケットであるか、個別制御パケットであるかによって処理を分岐させる。上記3種類のいずれでもなかった場合はセンターヘエラーを出力して終了する（ステップS206）。

【0086】

PPV受信履歴回収パケットは、例えば、チャレンジパケットの一形態と考えるても良く、PPV受信履歴回収のためのチャレンジ番号を割り振る方法でも実現できる。ここでは簡単のため、PPV受信履歴回収パケットは、PPV受信履歴回収のためのチャレンジ番号を割り振ったチャレンジパケットとする。

【0087】

受信パケットがPPV受信履歴回収以外のチャレンジパケットであった場合（図22のステップS203）、個別制御パケットであった場合（図22のステップS205）は第2の実施形態と同様の処理を行う。以下、受信パケットがPPV受信履歴回収パケットであった場合（図22のステップS204）について、図23に示すフローチャートを参照して説明する。

【0088】

センター間通信解析部151は、受信パケットがPPV受信履歴回収パケットであった場合、PPV受信管理部171に対してPPV受信履歴を回収する旨を指示する。PPV受信管理部171は、PPV受信履歴格納部172を検索して、未回収の受信履歴が存在すれば（ステップS211）、その受信履歴をレスポンスパケットに変換して（例えば、受信履歴を図18のレスポンスパケットの情

報本体となるように、レスポンスパケットを作成して) センター間通信解析部 1 5 1 へ送信し、センター間通信解析部 1 5 1 ではセンター間通信部 1 5 2 を経由してセンターへ送信する(ステップ S 2 1 2、ステップ S 2 1 3)。未回収の受信履歴が存在しなかった場合には、その旨のレスポンスパケットを生成してセンターへ送信する(ステップ S 2 1 1、ステップ S 2 1 6、ステップ S 2 1 7)。

【 0 0 8 9 】

センターでは、これを受信して P P V 受信履歴が存在した場合には受領を送信する(ステップ S 2 1 4)。受領を受けて受信装置の P P V 受信管理部 1 7 1 では、当該送信した P P V 受信履歴に対し、回収済みの処理を行う(ステップ S 2 1 5)。

【 0 0 9 0 】

このような P P V 受信履歴の回収のためのチャレンジパケットの送信を個別制御パケットの送信に先立て行うことにより、契約情報(チャンネル契約情報とワーク鍵等)の更新と同時に P P V 受信履歴を回収することが可能になる。更に、センターから送信される P P V 受信履歴の受領通知にデジタル署名を付けるなど安全対策を施せば、P P V 受信履歴をセンターに送信する前に受信装置に何らかの方法で受領情報を入力して、未回収の P P V 受信履歴を回収済みにしてしまうような攻撃にも耐えられる。

【 0 0 9 1 】

以上の第 1 ~ 第 3 の実施形態において主要な処理を限定受信部 1 0 0 の中だけで行っているが、デスクランブル部 1 2 0 のみを限定受信部 1 0 0 の外側で実装するという考え方もある。デスクランブル部 1 2 0 は(放送コンテンツを復号するのであるから)リアルタイムに復号しなくてはならないため高速処理が必要である一方、その他の部分は常に動作しなくてはならない部分は少なく、しかも処理時間に多少の余裕があるため実装上このようにすると有利なことが多い。例えば、他の放送との受信装置の共通化を図る際、全ての放送で放送コンテンツのスクランブル方式を共通にして、(各放送で秘密情報を保持したい)限定受信部分のみを I C カードなど脱着可能なメディア上に実装する実装方法が考えられる。

【 0 0 9 2 】

以上説明した第1～第3の実施形態、及びこれから述べる第4の実施形態においては、以上のような実装も可能であることを付け加えておく。

【0093】

（第4の実施形態）

第4の実施形態では、全ての放送受信装置が共通のマスター鍵を有する場合の限定受信システムについて説明する。第4の実施形態における限定受信システムはマスター鍵が全ての受信装置で共通であるため、第1の実施形態におけるワーク鍵の役割を（全受信装置に共通の）マスター鍵が果たしているので、図25に示すように、ワーク鍵が存在しない簡単な構造になっている。このような限定受信システムは構成が単純なため（放送波での送信を前提にした場合）、個別制御情報の送信量削減の点で大変有用である（特開平11-243536号公報参照）。しかし、マスター鍵が共通であるため、どの受信装置にも等しく全てのチャンネルのチャンネルキーが受信されてしまうため限定受信を実現するためにはチャンネル契約情報のみに依存することになる。

【0094】

本実施形態に係る放送受信装置の要部の構成例を図24に示す。第4の実施形態で用いられる個別制御パケットは図7で示した構成のパケットであるが、第4の実施形態においてはワーク鍵が存在しないので、個別制御パケットに暗号化されて載せられる契約情報は図26に示すような受信装置IDとチャンネル契約情報とデジタル署名とから構成される。

【0095】

共通制御パケットとしては、チャンネルキー情報を配信するためのパケットとマスター鍵生成情報を配信するためのパケットの2種類がある。チャンネルキーを配信するためのパケットは第1の実施形態の場合（図8参照）と同様、図27（a）に示す構成をしており、マスター鍵生成情報を配信するためのパケットは図27（b）に示すように、情報識別子、マスター鍵識別子、マスター鍵生成情報、デジタル署名からなっている。図27（b）において、情報識別子は当該パケットがマスター鍵生成情報を配信するためのパケットであることを示す識別子で、他のパケットと区別するために用いられる。マスター鍵識別子は続くマスター鍵

生成情報から生成されるマスター鍵の識別子である。デジタル署名は当該マスター鍵生成情報の偽造を防止するためのものであり、第 1 の実施形態で用いているデジタル署名と同様に秘密鍵暗号によるもの、公開鍵暗号によるものがあり、どちらを使ってもよい。

【 0 0 9 6 】

次に第 4 の実施形態に係る放送受信装置の処理動作について、第 1 の実施形態の場合と異なる部分についてのみ説明する。すなわち、共通制御パケットの受信処理動作が異なり、以下、図 2 8 に示すフローチャートを参照して説明する。

【 0 0 9 7 】

図 2 8 に示すフローチャートは、受信装置が共通制御パケットを受信し、フィルタ部 1 1 6 が当該受信した共通制御パケットを共通制御情報復号部 1 1 7 へ渡した時点から開始される。まず、受信パケットの情報識別子を参照して当該パケットがチャンネルキー配信用のものであるか判定する（ステップ S 3 0 1）。チャンネルキー配信用のパケットであれば、当該パケットの未暗号部分からマスター鍵識別子を取り出し、当該マスター鍵識別子を有するマスター鍵をマスター鍵格納部 1 0 3 から取得する（ステップ S 3 0 2）。取得したマスター鍵を使って受信したパケットの暗号化部分を復号する（ステップ S 3 0 3）。復号した結果得られたチャンネルキーをチャンネルキー格納部 1 1 8 へ格納し、終了する（ステップ S 3 0 4）。

【 0 0 9 8 】

一方、受信したパケットがマスター鍵生成情報配信用のパケットであれば（ステップ S 3 0 5）、当該パケットから取り出したマスター鍵識別子に対応したマスター鍵がマスター鍵格納部 1 0 3 に存在するか否かを判定する（ステップ S 3 0 6）。既に存在する場合はそこで終了する。存在しない場合は次に新しいマスター鍵の生成を行う。まず、マスター鍵生成情報検証部 1 8 1 は、当該パケットに含まれるデジタル署名を検証し（ステップ S 3 0 7）、検証失敗した場合は終了、検証成功した場合はマスター鍵生成部 1 8 2 で、当該パケットに含まれるマスター鍵生成情報から予め定められたアルゴリズムに従ってマスター鍵を生成し（ステップ S 3 0 8）、その生成されたマスター鍵をマスター鍵格納部 1 0 3 に

格納して終了する（ステップ S 3 0 9）。

【 0 0 9 9 】

ここで、マスター鍵生成情報とマスター鍵生成処理の説明を少ししなくてはならない。マスター鍵生成情報とは例えばマスター鍵生成のための乱数シード情報であり、乱数シードとマスター鍵生成部 1 8 2 の予め定められたアルゴリズムとパラメータによる乱数生成の手段によりマスター鍵を生成するものである。生成は耐タンパハードウェアの中で行われるため、マスター鍵生成情報は未暗号化のままでも安全上の問題はない。

【 0 1 0 0 】

（第 5 の実施形態）

第 5 の実施形態では、第 1 の実施形態で説明した放送受信装置に個別制御情報（パケット）を送信する情報配信装置（契約管理センター装置あるいは契約管理装置とも呼ぶ）について説明する。本発明においては、個別制御パケットと共通制御パケットとを別個の通信手段で送信することが本質的なので、情報配信装置に関しても個別制御パケット送信用と共通制御パケット送信用との 2 つに分けて説明する。実際このように構成することによって限定受信管理の複雑さも少なくなるため安定なシステムを築くことができる。

【 0 1 0 1 】

まず、個別制御パケットの情報配信装置の構成とその処理動作について説明する。図 2 9 は、情報配信装置の要部の構成例を示したもので、図 3 2 は、個別制御パケットの送信処理動作を示したフローチャートである。

【 0 1 0 2 】

加入者データベース（DB）2 0 2 には、各加入者毎の契約状態を管理するための加入者データを格納するもので、1 件の加入者データの構成は、図 3 1 に示すように、加入者 ID、受信装置 ID、マスター鍵識別子、マスター鍵、チャネル契約情報、送信済みフラグ、発呼番号からなっている。

【 0 1 0 3 】

加入者 ID とは加入者に対して付加した管理番号のことで、本実施形態では簡単のため「1」から「MAX ID」までの番号がふられているとする。受信装置

IDは加入者IDに示す加入者の受信装置IDを示している。マスター鍵識別子は当該加入者の受信装置の内部に現在存在するマスター鍵の識別子であり、マスター鍵は当該マスター鍵識別子に対応したマスター鍵である。チャンネル契約情報は当該加入者の契約状態を表す図2に示したような情報で、送信済みフラグは当該加入者に当該チャンネル契約情報を送信したか否かを示すフラグであり、「0」の時未送信、「1」の時は送信済みとなる。また、発呼番号は、例えば、当該加入者の受信装置に接続されている公衆電話回線の電話番号である。なお、この加入者データは、契約内容情報入力部201から入力されたデータで構成されている。

【0104】

以下、図32に示すフローチャートを参照して、図29の情報配信装置の個別制御パケットの送信処理動作について説明する。この処理は、ワーク鍵更新の都度、定期的に個別制御情報制御部206によって起動され、まず、変数*i* = 1とし、加入者IDが*i*である加入者レコードが加入者DB202内に存在するか否かをチェックする（ステップS301、ステップS302）。

【0105】

存在しなかった場合の処理を述べる。存在しなかった場合は、ステップS313に進み、*i*を1つインクリメントし、*i*が「MAXID」を越えないことを確認した上で（ステップS314）、ステップS302に戻り、新しい*i*で加入者IDをチェックする。ステップS314で変数*i*がMAXIDを越えてしまったら、全ての加入者データについて一通りの処理が終了したことを意味するので、加入者DB202を全検索して、送信済みフラグが「1」でない未送信の加入者データが存在するか否かを検査し（ステップS315）、未送信の加入者データがあれば、ステップS301に戻り、変数*i* = 1にして処理を最初から行う。ステップS315で未送信の加入者データがなければ終了する。

【0106】

変数*i*がMAXIDを越えるまで*i*をインクリメントして当該変数*i*を加入者IDとする加入者データが存在するか否かをチェックする（ステップS302）。存在した場合、当該加入者データの送信済みフラグを参照して、「1」であれ

ば送信済みなので（ステップS303）、iを1つインクリメントして（ステップS313～ステップS314）、加入者IDの存在チェックに戻る（ステップS302）。尚、本処理（ステップS302、ステップS303、ステップS313～ステップS314）は以下でも度々現れる処理であるので、以下の説明では簡単のためインクリメント処理と呼ぶことにする。

【0107】

ステップS302で加入者ID=iの加入者データが存在した場合、当該加入者データの送信済みフラグを参照して（ステップS303）、「1」であれば送信済みなので、ステップS313に進みiを1つインクリメントして、加入者IDの存在チェックに戻る（ステップS314、ステップS302）。

【0108】

ステップS303で送信済みフラグが「0」であった時は、個別制御情報制御部206は、当該加入者データのチャンネル契約情報に基づいて、当該加入者が視聴できるチャンネルのワーク鍵をワーク鍵データベース（DB）204から取得する（ステップS304）。ここでワーク鍵は（第1の実施形態でも説明したように）チャンネル毎に設定されていると仮定しているのでこのように契約チャンネル分だけのワーク鍵を取得する処理が必要になる。

【0109】

個別制御情報作成部203は、取得されたワーク鍵と当該加入者データの受信装置ID、チャンネル契約情報からデジタル署名以外の図5に示したような構成の契約情報本体を作成し、この契約情報本体をデジタル署名生成鍵格納部205に格納されているデジタル署名生成鍵を用いて暗号化してデジタル署名を作成し、それを暗号化された契約情報本体に付加して図5に示したような契約情報を作成する。更に当該加入者レコードのマスター鍵で契約情報を暗号化し、マスター鍵識別子や情報識別子を付加して個別制御パケットを作成する（ステップS305）。作成されたパケットは、送受信制御部207に送られ、送受信制御部207は、当該加入者データに含まれている発呼番号で発呼を行う（ステップS306）。この発呼を当該受信装置が受信しなかった場合は受信エラーを出力して（ステップS307、ステップS308）、ステップS313に進み、インクリメン

ト処理を行って、次の加入者データに処理を移す。

【0 1 1 0】

発呼に対して当該受信装置が受信した場合、送受信制御部 2 0 7 は予め定められたプロトコルによって個別制御パケットを送信する（ステップ S 3 0 7）。送信後、一定期間に当該受信装置より受領通知があった場合（ステップ S 3 1 0）、当該加入者データの送信済みフラグを「1」にして（ステップ S 3 1 2）、ステップ S 3 1 3 以降のインクリメント処理を行ったのち、次の加入者レコードに処理を移す。

【0 1 1 1】

上記処理は変数 i が「MAX ID」を越え、全ての加入者データが送信済みであることを確認した時点で終了する（ステップ S 3 1 5）。

【0 1 1 2】

次に、共通制御パケットの情報配信装置の構成とその処理動作について説明する。図 3 0 は、情報配信装置の要部の構成例を示したもので、図 3 4 は、共通制御パケットの送信処理動作を示したフローチャートである。この処理は、放送開始と同時に開始され、放送が続く間間断なく繰り返される。まず $i = 1$ とし（ステップ S 3 2 1）、チャンネル ID = i であるようなチャンネルキーデータが存在するか、チャンネルキーデータベース（DB）3 1 2 をチェックする（ステップ S 3 2 2）。

【0 1 1 3】

チャンネルキー DB 3 1 2 には、各チャンネル毎のチャンネルデータが登録されていて、1つのチャンネルキーデータは、図 3 3 に示すように、チャンネル ID とチャンネル識別子、チャンネルキー識別子（1）、チャンネルキー（1）、チャンネルキー識別子（2）、チャンネルキー（2）から構成されている。ここでチャンネル ID とは各チャンネルに付されるデータベース管理上の番号で、本実施形態では「1」から MAX ID までの値を取るものとする。チャンネル識別子は受信装置が各チャンネルを識別するための情報で第 1 ～ 第 4 の実施形態で説明したそれと同じである。更にチャンネルキー識別子及びチャンネルキーも第 1 ～ 第 4 の実施形態で述べたものと同じである。ここで 2 組のチャンネルキーが存在するのは現在有効なチャンネルキ

ーと次に使われるチャンネルキーと一緒に送信する必要があるためであり、構成によっては現在使用されているチャンネルキーのみでも構わない。

【 0 1 1 4 】

さて、ここでチャンネルIDが*i*のチャンネルキーデータが無かった場合は、ステップS325へ進み、*i*を1つインクリメントして、*i*が「MAXID」を越えなければ（ステップS326）、ステップS322に戻り、チャンネルIDチェックに戻る。さもなくば、チャンネル送信が一周り終了したことを意味するので、ステップS321に戻り、*i* = 1にしてチャンネルデータチェックから開始する。

【 0 1 1 5 】

以下、ステップS322で、チャンネルIDが*i*であるチャンネルキーデータがあった場合を考える。この場合、共通制御情報作成部313は、当該チャンネルデータからチャンネル識別子、チャンネルキー識別子（1）、チャンネルキー（1）、チャンネルキー識別子（2）、チャンネルキー（2）を取得する。また、チャンネル識別子あるいはチャンネルIDをキーにしてワーク鍵DB311を検索し、当該チャンネルの有効なワーク鍵を抽出し、当該ワーク鍵を使って共通制御パケット内のデータのうち暗号化すべき部分を暗号化する。更に、当該ワーク鍵のワーク鍵識別子と情報識別子を付けて共通制御パケットを生成し、送信部315へ渡す（ステップS324）。送信部315は、この生成された共通制御パケットを放送波に載せて発信する。

【 0 1 1 6 】

以上第5の実施形態では、個別制御パケットを公衆電話等の双方向通信手段で送信することによって、放送帯域に占める制御情報の情報量を減らせるばかりか、個別制御パケットの受信状況を情報配信装置側で把握することができる。このように個別制御パケットと共通制御パケットの性格に鑑み、送信形態を変えることで、放送帯域の確保及び限定受信システムの安全性の向上に貢献できる。

【 0 1 1 7 】

（第6の実施形態）

次に、いくつかのバリエーションを述べる。第1のバリエーションとして、チャレンジアンドレスポンスの手法によって、送信側で受信装置の正当性を確かめ

るという第2の実施形態で述べた放送受信装置に対応する情報配信装置（契約管理センター装置あるいは契約管理装置とも呼ぶ）がある。

【0118】

また、第2のバリエーションとしては、契約管理センターから公衆回線を使って個別制御パケットを送信する際、個別制御パケットを送信する前にPPV（ペイパービュー）の受信履歴の回収を行う限定受信システムに用いられる情報配信装置（契約管理センター装置あるいは契約管理装置とも呼ぶ）がある。

【0119】

ここでは第1のバリエーション及び第2のバリエーションの両方を実現できる情報配信装置の構成とその処理動作について説明する。

【0120】

図35は、第6の実施形態に係る情報配信装置の要部の構成例を示したもので、以下、図36～図38に示すフローチャートを参照して図35に示した情報配信装置の処理動作について説明する。この処理は、契約更新期間を考慮して、適切な時期（例えば、1ヶ月毎）に起動される。まず、制御部221は、 $i = 1$ として（ステップS401）、加入者ID= i となるような加入者IDを持つ加入者データがあるか否かを加入者DB202を検索してチェックする（ステップS402）。存在しない場合は第5の実施形態で説明したインクリメント処理を行い、次の加入者データへ処理を移す。ステップS402で加入者データが存在した場合は、当該加入者データの送信済みフラグを参照し、「0」であった場合は受信装置IDと発呼番号を当該加入者データから取得し、送受信制御部207から当該発呼番号を用いて受信装置を発呼する（ステップS404～ステップS405）。この発呼に対し、受信装置が応答（受信）しない場合（ステップS406）、受信不良の旨のエラー出力をする（ステップS434）。

【0121】

応答があった場合は、ステップS407へ進み、制御部221からチャレンジ作成部222に対して受信装置IDを尋ねるチャレンジの作成を要請し、チャレンジ作成部222ではチャレンジデータベース（DB）224を参照し、当該チャレンジパケットを作成する。

【 0 1 2 2 】

ここでチャレンジDB 2 2 4 とは各種チャレンジのチャレンジ番号と処理の組が記載されたデータベースである。ここではチャレンジ作成部 2 2 2 がチャレンジDB 2 2 4 から受信装置IDを問い合わせるチャレンジ番号をキーにして処理内容を抽出する。作成されたチャレンジパケットは制御部 2 2 1 を経由して送受信部 2 0 7 に送られ、ここから受信装置に送信される（ステップS 4 0 7）。

【 0 1 2 3 】

送信後一定期間内に受信装置から応答が無かった場合、受信装置IDを問い合わせるチャレンジ失敗の旨のエラー出力し（ステップS 4 3 5）、ステップS 4 3 2 へ進み、インクリメント処理を行ない、次の加入者レコードの処理に移行する（ステップS 4 3 3、ステップS 4 0 2）。応答があった場合、そのレスポンスパケットを送受信部 2 0 7、制御部 2 2 1 を経由してレスポンス検査部 2 2 3 に送り、レスポンス検査部 2 2 3 において加入者データ中の受信装置IDと一致するか検査する（ステップS 4 0 9）。ここで一致しなかった場合は受信装置ID不一致の旨のエラー出力をし（ステップS 4 3 6）、ステップS 4 3 2 へ進みインクリメント処理の後、次の加入者レコードの処理に移る。

【 0 1 2 4 】

ステップS 4 0 9 において、レスポンス検査部 2 2 3 で正しいレスポンスが得られたことが確認できたら、次に、前述同様マスター鍵識別子を尋ねるチャレンジを行い、そのレスポンスを検査する（ステップS 4 1 0～ステップS 4 1 2）。加入者データ中のマスター鍵識別子とレスポンスとして送られてきたマスター鍵識別子が一致していなかった場合は、マスター鍵識別子不一致の旨のエラー出力を行い（ステップS 4 3 8）、インクリメント処理の後、次の加入者データに処理を移す。一致していた場合は、図 3 7 のステップS 4 1 3 へ進み、以下に説明する受信装置認証の処理を行う。

【 0 1 2 5 】

受信装置認証処理は、正当な受信装置しか知らない情報を使って答えさせるチャレンジを1つ以上発生させ、そのレスポンスで認証を行う処理である。まず制御部 2 2 1 で変数「j」に「1」を設定し（ステップS 4 1 3）、チャレンジ作成部

2 2 2 に対して認証チャレンジを発行するように要請する。要請を受けたチャレンジ作成部 2 2 2 ではチャレンジ DB 2 2 4 からランダムにチャレンジを抽出し、チャレンジパケットを作成し、制御部 2 2 1 へ渡す（ステップ S 4 1 4）。このチャレンジパケットは送受信部 2 0 7 を経由して受信装置に送信される（ステップ S 4 1 5）。送信後一定期間内に受信装置から応答が無かった場合（ステップ S 4 1 6）、当該チャレンジ失敗の旨のエラー出力を行い（ステップ S 4 3 9）、インクリメント処理を行なって（ステップ S 4 3 2、ステップ S 4 3 3）、次の加入者レコードの処理に移行する。

【 0 1 2 6 】

応答があった場合、そのレスポンスパケットを送受信部 2 0 7、制御部 2 2 1 を経由してレスポンス検査部 2 2 3 に送り、レスポンス検査部 2 2 3 においてチャレンジ DB 2 2 4 に定められた認証アルゴリズムによって認証検査を行う（ステップ S 4 1 7）。認証検査が成功した場合は正しいレスポンスであることが示されたので、ステップ S 4 1 8 に進み、j を 1 つインクリメントして j が N を越えるか否かチェックする（ステップ S 4 1 9）。N は予めシステムに依存した定数で、認証チャレンジの試行回数を意味する。j が N を越えない場合、j が N を越えるまで前記認証処理を繰り返す。

【 0 1 2 7 】

ステップ S 4 1 7 で認証検査が失敗した場合は間違ったレスポンスであるので、認証失敗の旨のエラー出力を行い（ステップ S 4 4 0）、インクリメント処理の（ステップ S 4 3 2、ステップ S 4 3 3）後、次の加入者データの処理に移る。

【 0 1 2 8 】

以上の認証処理の結果、j が N を越えた場合は（ステップ S 4 1 9）、認証が終了したことを意味し、情報配信装置側で現在通信を行っている受信装置が正当なものであることを確認できたことになる。そこで、次に PPV 受信履歴の回収処理を行う。まず、制御部 2 2 1 は PPV 受信履歴回収パケットを生成する旨の要請をチャレンジ作成部 2 2 2 に要請する。チャレンジ作成部 2 2 2 ではチャレンジ DB 2 2 4 を参照するなどして PPV 受信履歴回収のためのチャレンジパケット（PPV 受信履歴回収パケット）を作成し、制御部 2 2 1 に渡す（ステップ S 4

20)。制御部221ではチャレンジパケットを受送信部207、モデム208経由で受信装置に送信する(ステップS421)。送信後一定期間待った後、応答が無かった場合はPPV受信履歴回収の応答がなかった旨のエラー出力を行い(ステップS422、ステップS441)、インクリメント処理(ステップS432、ステップS433)の後、次の加入者データに処理を移す。

【0129】

応答があった場合、受信したレスポンスパケットを制御部221経由でレスポンス検査部223へ渡す。レスポンス検査部223では当該レスポンスパケットに対する形式的な検査と受信履歴が存在するかどうかの検査を行う(ステップS423)。PPV受信履歴が存在した場合は、制御部221に当該受信履歴を渡し、制御部221は、それをPPV受信履歴データベース(DB)225に格納する(ステップS424)。ここでは詳しく述べないが、後日この受信履歴に基づいて加入者に視聴料金の徴収が行われる。

【0130】

一方、制御部221はDB225にPPV受信履歴が登録されたことを確認した後、PPV受信履歴受領パケットを作成し、受信装置に送信する(ステップS425)。なお、ステップS423でPPV受信履歴が存在しなかった場合は、ステップS424～ステップS425の処理をスキップする。

【0131】

PPV受信履歴の回収処理が終了した後、制御部221は個別制御情報作成部203に当該加入者データの個別制御パケットを作成するように要請する。個別制御情報作成部203ではこれを受けて、当該加入者データのチャンネル契約情報に基づいて当該加入者が視聴できるチャンネルのワーク鍵をワーク鍵DB204から取得する(ステップS426)。ここでは、ワーク鍵はチャンネル毎に設定されていると仮定しているので、このように契約チャンネル分だけのワーク鍵を取得する処理が必要になる。

【0132】

次に取得されたワーク鍵とワーク鍵識別子のペア及び当該加入者データの受信装置ID、チャンネル契約情報からデジタル署名以外の契約情報本体を作成しさら

に、デジタル署名生成鍵を用いて、図 5 に示すような契約情報を作成する。更に当該加入者データのマスター鍵で契約情報を暗号化し、マスター鍵識別子や情報識別子を付加して、図 7 に示したような個別制御パケットを作成する（ステップ S 4 2 7）。

【 0 1 3 3 】

この作成されたパケットは制御部 2 2 1 を経由して送受信部 2 0 7 へ送られ、受信装置へ送信される（ステップ S 4 2 8）。当該送信後、一定期間に受信装置より受領通知があった場合は（ステップ S 4 2 9）、当該加入者データの送信済みフラグを「1」にして（ステップ S 4 5 0）、インクリメント処理を行ない（ステップ S 4 3 2、ステップ S 4 3 3）、次の加入者データへ処理を移す。受領通知がなかった場合は（ステップ S 4 2 9）、個別制御パケット受領失敗の旨のエラー出力を行い（ステップ S 4 4 2）、インクリメント処理（ステップ S 4 3 2、ステップ S 4 3 3）を行った後、次の加入者データへ処理を移す。全ての加入者データが送信済みとなった時点で（ステップ S 4 3 1）、全体の処理も終了する。

【 0 1 3 4 】

以上説明したように、第 6 の実施形態によれば、受信装置の正当性を認証した後、P P V 受信履歴の回収や個別制御パケットの送信が行えるため、不正視聴を防止できるという意味で安全性に優れた限定受信システムを構築できる。特に P P V 受信履歴は従来加入者側で電話線を外せるため回収困難となる場合もあったが、本実施形態によれば、P P V 受信履歴回収の後、個別制御情報の更新となるので、P P V 受信履歴の回収がない場合には一般の放送までも視聴不可能になってしまう。逆に言うと、本実施形態においては処理の順番は本質的であり、特に P P V 受信履歴の回収は個別制御情報の更新に先だって行なう必要がある。

【 0 1 3 5 】

以上の説明からも明らかなように本実施形態を部分的に実施した実施形態も成立し得る。例えば、P P V 受信履歴の回収を省略することができる。実際、P P V サービスを行わない放送事業に関しては本実施形態は P P V 受信履歴の回収を省略して実施されることになる。この場合でも本実施形態によって受信装置の正

当性を認証する上で効果があり、これが第1のバリエーションであった。一方、受信装置の認証を省略する実施形態も可能である。この場合でもPPV受信履歴の回収を更新すべき個別制御情報の送付に先だって行うことにより、PPV受信履歴の回収を確実にする効果があり、これが第2のバリエーションであった。以上で第1、第2のバリエーションの説明を終了する。

【0136】

(第7の実施形態)

次に第3のバリエーションを述べる。第3のバリエーションでは個別制御パケットの受信の可否によって視聴料金請求額を変更する実施形態について述べる。加入者が契約を変更する（例えば、視聴するチャンネルを変更する等）際、従来は変更の申し出があった月もしくは翌月から（受信装置側でチャンネル契約情報が変更されたかどうかに関わらず）変更された契約内容に沿って視聴料を徴収していた。本実施形態では視聴料請求をより実質の視聴形態に近づけるため、受信装置側を契約変更に伴う契約情報に更新するための個別制御パケットを当該受信装置にて受信されたか否かによって視聴料請求金額の変更を決定しようとするものである。このように構成することによって、例えば、全てのチャンネルの契約を解除した後の無料視聴されることを防止できる。

【0137】

第7の実施形態に係る個別制御情報の情報配信装置は、図29に示した第5の実施形態に係る情報配信装置と同様である。ただし、第7の実施形態の場合は、加入者DB202の加入者レコードが異なる。すなわち、図39に示すように、加入者データは、図31に示した現在のチャンネル契約情報に代えて、視聴チャンネル変更（契約変更）前の旧チャンネル契約情報と視聴チャンネル変更（契約変更）後の新チャンネル契約情報を含み、さらに、視聴有効フラグが付加されている。

【0138】

旧チャンネル契約情報とは、変更前の当該受信装置のチャンネル契約情報であり、新チャンネル契約情報は変更後のチャンネル契約情報である。但し、新規に当該有料放送サービスに加入した場合の新規加入者に対しては、新チャンネル契約情報にその契約時の指定したチャンネルに対応したビットが「1」であるチャンネル契約情報

が入り、旧チャンネル契約情報には（無料チャンネル以外の）全てのチャンネルに対応したビットが「0」であるチャンネル契約情報が入る。また、視聴有効フラグは新チャンネル契約情報が受信装置に反映されたかどうか（当該受信装置に格納されているチャンネル契約情報が新チャンネル契約情報に更新されているか否か）を示す1ビットのデータで、「1」の時、新チャンネル契約情報が有効、「0」の時、旧チャンネル契約情報が有効であることを意味する。

【0139】

本実施形態の処理に関しては、第5の実施形態の図32とほぼ同様であるが、ステップS310で個別制御パケットの受領があった場合、ステップS312で当該加入者レコードの送信済みフラグを「1」にすると同時に視聴有効フラグも「1」にして、加入者DB202の上でもそれを反映する処理が加わる点が異なる。このようにすることで、センターにある加入者DB202上で実際の受信装置側で現在有効となっている（契約情報格納部121に格納されている）チャンネル契約情報を知ることができるので実際有効となっているチャンネル契約情報を基に視聴料請求時に請求額を変更することが可能となる。実際、従来の実施形態もしくは第5の実施形態では受信装置内部もチャンネル契約情報の状態に関わらず一律に新しい契約形態で料金を徴収することになるのに対し、第7の実施形態を用いることによって、より実際の契約形態に近い視聴料請求が実現されるため、無料視聴を防止できるばかりか、実際に受信していないチャンネル契約情報に対して視聴料金が徴収されることによる加入者からのクレームを避けることができる。

【0140】

（第8の実施形態）

第8の実施形態は、第4の実施形態で説明した放送受信装置に個別制御パケットを送信する情報配信装置について説明する。第8の実施形態に係る情報配信装置は、図29に示す第5の実施形態に係る情報配信装置の構成および処理動作の説明に重複する部分が多いので異なる部分のみを説明するに留める。

【0141】

また、第1の実施形態に係る放送受信装置と第4の実施形態に係る放送受信装置とでは、個別制御パケットのデータ構成に若干の違いはあっても（第4の実施

形態に係る個別制御パケットに含まれる契約情報にはワーク鍵が含まれていない)、その取り扱いは同様である。すなわち、図 3 2 において、ワーク鍵を取得するステップ S 3 0 4 をスキップしてステップ S 3 0 5 で個別制御パケットを作成すればよい。

【 0 1 4 2 】

そのため第 8 の実施形態における個別制御パケットの情報配信装置は、第 5 の実施形態における情報配信装置の構成からワーク鍵 DB 2 0 4 が除かれる以外は、図 2 9 と同様である。

【 0 1 4 3 】

このことから以下、共通制御パケットの情報配信装置に絞って説明する。共通制御パケットに関して第 1 の実施形態ではチャンネルキーの情報のみが共通制御パケットとして送信されていたのに対し、第 4 の実施形態では共通制御パケットとしてチャンネルキーとマスター鍵生成情報の 2 つがそれぞれ別個のパケットにて送信されていた。このため第 8 の実施形態では、この 2 種類の共通制御パケットを作成していかななくてはならないところが第 5 の実施形態と本質的に異なる。

【 0 1 4 4 】

第 8 の実施形態に係る情報配信装置の構成図を図 4 0 に、その処理動作を図 4 1 に示す。以下、図 4 0 を参照しながら図 4 1 に基づき説明する。

【 0 1 4 5 】

図 4 1 の処理は、放送開始時に開始され、放送が終了するまで中断なく継続される。まず、チャンネルキー配信用パケット作成部 3 5 5 は、共通制御情報制御部 3 1 4 から処理開始の指示を受けると、 $i = 1$ とし (ステップ S 5 0 1)、チャンネル ID = i であるようなチャンネルキーデータが存在するかを、チャンネルキー DB 3 1 2 を検索してチェックする (ステップ S 5 0 2)。ここでチャンネル ID が i のチャンネルキーが存在した場合、当該チャンネルキーデータからチャンネル識別子、チャンネルキー識別子 (1)、チャンネルキー (1)、チャンネルキー識別子 (2)、チャンネルキー (2) を取得し (ステップ S 5 0 3)、チャンネルキー配信用の共通制御パケットの一部を作成する。更にマスター鍵格納部 3 5 1 から現在有効なマスター鍵を抽出し、当該マスター鍵を使って、図 2 7 に示したチャンネルキー配

信用の共通制御パケットの暗号化されるべき部分（チャンネル識別子からチャンネルキー（2）までの部分）を暗号化する。更に、チャンネルキー配信用の共通制御パケットを暗号化する際に用いたマスター鍵のマスター鍵識別子とチャンネルキー配信用の共通制御パケットである旨を識別するための情報識別子を付けて共通制御パケットを生成し（ステップS504）、情報送信部315へ渡す。情報送信部315では当該パケットを放送波に載せて発信する（ステップS505）。

【0146】

一方、ステップS502でチャンネルID=iであるチャンネルキーが存在しなかった場合は、ステップS506へ進み、iを1つインクリメントして、iが「MAXID」を越えなければ（ステップS507）、ステップS502のチャンネルIDチェックに戻る。iが「MAXID」を越えてしまった場合はチャンネルキー送信が一周り終了したことを意味するので、チャンネルキー送信を一旦中断し、ステップS508以降のマスター鍵生成情報の送信に処理を移す。

【0147】

共通制御情報制御部314からマスター鍵生成情報配信用パケット作成部354へパケット作成の要請があると、マスター鍵生成情報配信用パケット作成部354では、マスター鍵生成情報作成部353で作成された現在有効なマスター鍵生成情報と当該マスター鍵生成情報に対応したマスター鍵識別子を取得し（ステップS508）、図27（b）に示したようなマスター鍵生成情報配信用のパケットの構造に従って結合し、デジタル署名を付加する。更に情報識別子を付加してマスター鍵生成情報配信用の共通制御パケットを生成し（ステップS509）、情報送信部315へ渡し、情報送信部315では当該パケットを放送波に載せて発信する（ステップS510）。

【0148】

なお、マスター鍵生成情報作成部353は、定期的に、例えば公知の乱数生成手段により乱数シード情報としてのマスター鍵生成情報を作成し、マスター鍵作成部352は、受信装置側のマスター鍵生成部182と同じアルゴリズムを保持して、マスター鍵生成情報作成部353で作成されたマスター鍵生成情報と当該アルゴリズムとを用いて、現在有効なマスター鍵を生成するようになっている。

マスター鍵格納部 3 5 1 には、この現在有効なマスター鍵が生成されているものとする。

【 0 1 4 9 】

以上が第 8 の実施形態の説明であるが、本実施形態の要部は、容易に分かるように第 5 ～ 第 7 の実施形態で示した情報配信装置にも適用可能である。

【 0 1 5 0 】

(追記)

尚、チャンネル数が少ない放送においては、チャンネル契約情報を用いずに、ワーク鍵のみによる限定受信も可能である。実際、ワーク鍵は、チャンネル毎に設定されている鍵なので、このワーク鍵を契約期間（例えば 1 ヶ月）毎に更新し、更新されたワーク鍵を当該契約期間に当該チャンネルを視聴している視聴者のみに個別制御情報として送信することにより、契約者のみへの視聴限定ができる。

【 0 1 5 1 】

このような構成において、受信装置側は、当該チャンネルのチャンネルキーが共通制御パケットで送信されてきたとき、共通制御パケットのヘッダ部分に記載されているワーク鍵識別子をキーにして、当該チャンネルのワーク鍵がワーク鍵格納部に存在するかをチェックする。存在した場合には当該制御パケットの暗号化部を復号し、当該チャンネルのチャンネルキーを取得する。存在しなかった場合は当該共通制御パケットに対する処理を終了する。このことから当該チャンネルのワーク鍵を持っている当該チャンネルの視聴契約者だけが当該チャンネルキーを取得できるため、限定受信が実現できる。

【 0 1 5 2 】

このように、各チャンネルのワーク鍵を契約期間毎に更新するだけでも、限定受信システムは構成できる。ただし、現在の C S 放送のようにチャンネル数が多い場合、ワーク鍵を契約期間毎に変更するとワーク鍵の更新情報が大規模になるため現実的でない。それ故に現在の C S 放送においては上記第 1 ～ 第 8 の実施形態で説明したようなチャンネル契約情報を併用する方式が望ましい。しかし、例えば、1 チャンネルしかない（もしくは、契約形態が 1 つしかない）放送においては、ワーク鍵は 1 つで充分なので、上記のようなワーク鍵のみによる限定受信システ

ムもメリットがある。

【0153】

なお、第1の実施形態およびそれに関連する実施形態において、受信装置にて記憶されるチャンネル契約情報、ワーク鍵は、1つの個別制御パケットにて同時に更新してもよいし、どちらか一方のみを更新するようにしてもよい。

【0154】

また、第1～第8の実施形態において、デジタル署名を作成する際、デジタル署名の対象である情報部分とその特徴量としてのハッシュ値とを暗号化してデジタル署名を作成してもよい。すなわち、例えば、図5の契約情報中のデジタル署名であれば、デジタル署名以外の部分とそのハッシュ値とを暗号化して契約情報のデジタル署名を作成してもよい。

【0155】

なお、本発明は、上記第1～第8の実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。さらに、上記実施形態には種々の段階の発明は含まれており、開示される複数の構成要件における適宜な組み合わせにより、種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題（の少なくとも1つ）が解決でき、発明の効果の欄で述べられている効果（の少なくとも1つ）が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【0156】

【発明の効果】

以上説明したように本発明によれば、加入者が増加しても大量の個別制御情報を配信することにより放送帯域を圧迫することなく、さらに不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする。

【図面の簡単な説明】

【図1】

本発明の第1の実施形態に係る放送受信装置の要部の構成例を示した図。

【図2】

チャンネル契約情報の一例を示した図。

【図 3】

限定受信システムで用いられる鍵構成の一例を示した図。

【図 4】

コンテンツパケットのデータ構成の一例を示した図。

【図 5】

契約情報の一例を示した図。

【図 6】

チャンネル契約情報の他の例を示した図。

【図 7】

個別制御パケットのデータ構成の一例を示した図。

【図 8】

共通制御パケットのデータ構成の一例を示した図。

【図 9】

図 1 に示した放送受信装置の個別制御パケット受信処理動作を説明するためのフローチャート。

【図 1 0】

図 1 に示した放送受信装置の共通制御パケット／コンテンツパケットの受信処理動作を説明するためのフローチャート。

【図 1 1】

共通制御パケット／コンテンツパケットの受信処理動作を説明するためのフローチャート。

【図 1 2】

チャンネル選択／チャンネルキー取得処理動作を説明するためのフローチャート。

【図 1 3】

共通制御パケット／コンテンツパケットの受信処理動作を説明するためのフローチャート。

【図 1 4】

本発明の第 2 の実施形態に係る放送受信装置の要部の構成例を示した図。

【図 1 5】

第 2 の実施形態に係るパケットのデータ構成例を示した図。

【図 1 6】

個別制御パケットのデータ構成例を示した図。

【図 1 7】

チャレンジパケットのデータ構成例を示した図。

【図 1 8】

レスポンスパケットのデータ構成例を示した図。

【図 1 9】

個別制御パケットの受信処理動作を説明するためのフローチャート。

【図 2 0】

個別制御パケットの受信処理動作を説明するためのフローチャート。

【図 2 1】

本発明の第 3 の実施形態に係る放送受信装置の要部の構成例を示した図。

【図 2 2】

個別制御パケットの受信処理動作を説明するためのフローチャート。

【図 2 3】

個別制御パケットの受信処理動作を説明するためのフローチャート。

【図 2 4】

本発明の第 4 の実施形態に係る放送受信装置の要部の構成例を示した図。

【図 2 5】

第 4 の実施形態に係る限定受信システムで用いられる鍵構成の一例を示した図。

【図 2 6】

第 4 の実施形態に係る契約情報の一例を示した図。

【図 2 7】

共通制御パケットのデータ構成例を示した図で、（a）図はマスター鍵生成情報配信用の共通制御パケットの場合、（b）図はチャンネルキー配信用の共通制御パケットの場合を示している。

【図 2 8】

共通制御（パケットの受信処理動作を説明するためのフローチャート。

【図 2 9】

本発明の第 5 の実施形態に係る個別制御情報の情報配信装置であって、第 1 の実施形態に係る放送受信装置（図 1）に対応する情報配信装置の要部の構成例を示した図。

【図 3 0】

本発明の第 5 の実施形態に係る共通制御情報の情報配信装置であって、第 1 の実施形態に係る放送受信装置（図 1）に対応する情報配信装置の要部の構成例を示した図。

【図 3 1】

図 2 9 の加入者データベースに格納されている加入者データの一例を示した図。

【図 3 2】

個別制御パケットの送信処理動作を説明するためのフローチャート。

【図 3 3】

図 3 0 のチャンネルキーデータベースに格納されているチャンネルキーデータの一例を示した図。

【図 3 4】

共通制御パケットの送信処理動作を説明するためのフローチャート。

【図 3 5】

本発明の第 6 の実施形態に係る個別制御情報の情報配信装置であって、第 2 の実施形態に係る放送受信装置（図 1）に対応する情報配信装置の要部の構成例を示した図。

【図 3 6】

図 3 5 の情報配信装置の処理動作を説明するためのフローチャート。

【図 3 7】

図 3 5 の情報配信装置の処理動作を説明するためのフローチャート。

【図 3 8】

図 3 5 の情報配信装置の処理動作を説明するためのフローチャート。

【図 3 9】

本発明の第 7 の実施形態に係る個別制御情報（パケット）の情報配信装置で用いられる加入者データの一例を示した図。

【図 4 0】

本発明の第 8 の実施形態に係る共通制御パケットの情報配信装置であって、第 4 の実施形態に係る放送受信装置に対応する情報配信装置の要部の構成例を示した図。

【図 4 1】

図 4 0 の情報配信装置の共通制御パケットの送信処理動作を説明するためのフローチャート。

【符号の説明】

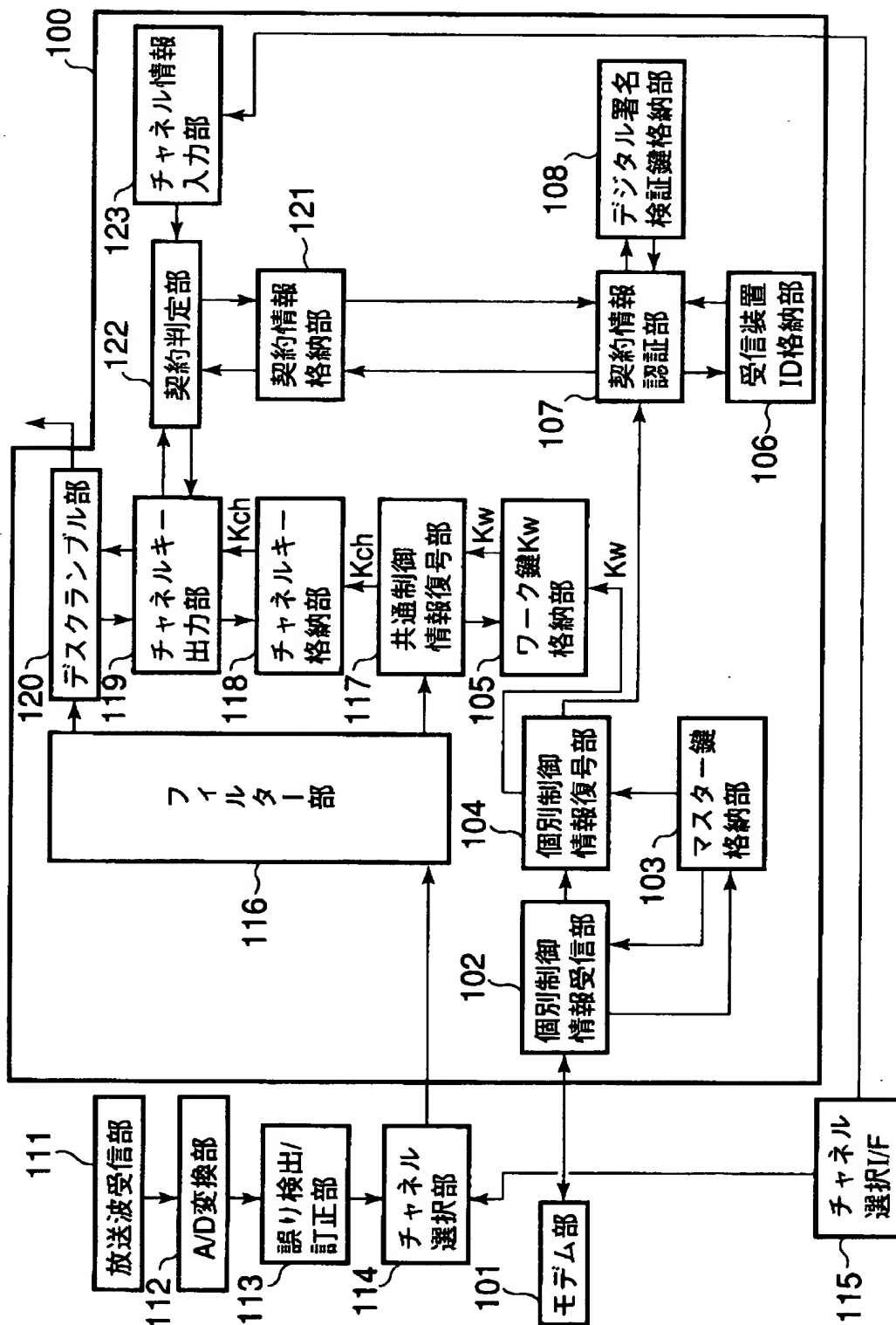
- 1 0 0 … 限定受信部
- 1 0 1 … モデム部
- 1 0 2 … 個別制御情報受信部
- 1 0 3 … マスター鍵格納部
- 1 0 4 … 個別制御情報復号部
- 1 0 5 … ワーク鍵格納部
- 1 0 6 … 受信装置 I D 格納部
- 1 0 7 … 契約情報認証部
- 1 0 8 … デジタル署名検証鍵格納部
- 1 1 1 … 放送波受信部
- 1 1 2 … A / D 変換部
- 1 1 3 … 誤り検出 / 訂正部
- 1 1 4 … チャンネル選択部
- 1 1 5 … チャンネル選択インタフェース（I / F）部
- 1 1 6 … フィルター部
- 1 1 7 … 共通制御情報復号部
- 1 1 8 … チャンネルキー格納部

- 1 1 9 …チャンネルキー出力部
- 1 2 0 …デスクランブル部
- 1 2 1 …契約情報格納部
- 1 2 2 …契約判定部
- 1 2 3 …チャンネル情報入力部
- 2 0 2 …加入者データベース
- 2 0 3 …個別制御情報作成部
- 2 0 4 …ワーク鍵データベース
- 2 0 5 …デジタル署名生成鍵作成部
- 2 0 6 …個別制御情報制御部
- 2 0 7 …送受信制御部
- 2 0 8 …モデム
- 3 1 1 …ワーク鍵データベース
- 3 1 2 …チャンネルキーデータベース
- 3 1 3 …共通制御情報作成部
- 3 1 4 …共通制御情報制御部
- 3 1 5 …送信部

【書類名】

図面

【図 1】

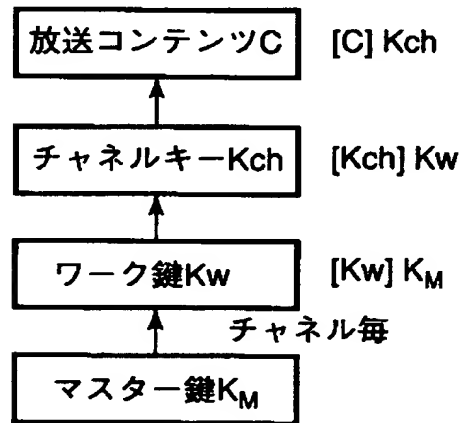


【図 2】

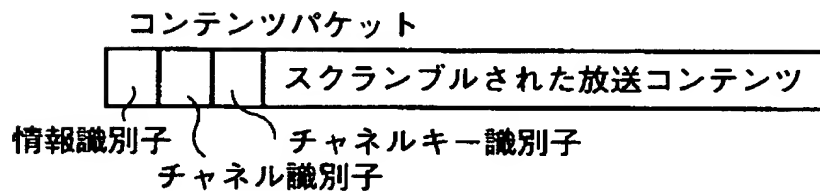
チャンネル契約情報

1	2	3	4	5	6	7	8
0	1	0	0	1	0	1	1

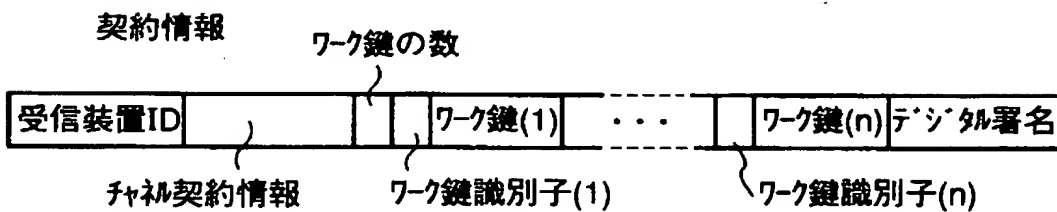
【図 3】



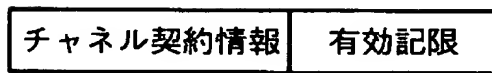
【図 4】



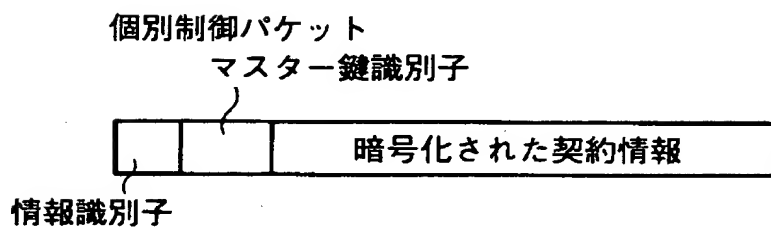
【図 5】



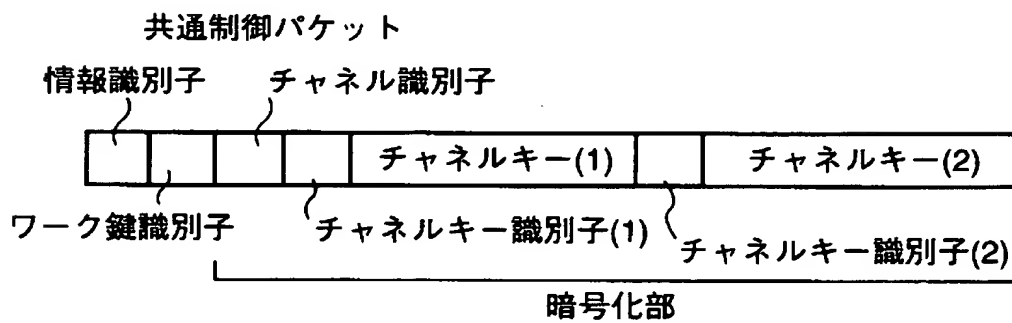
【図 6】



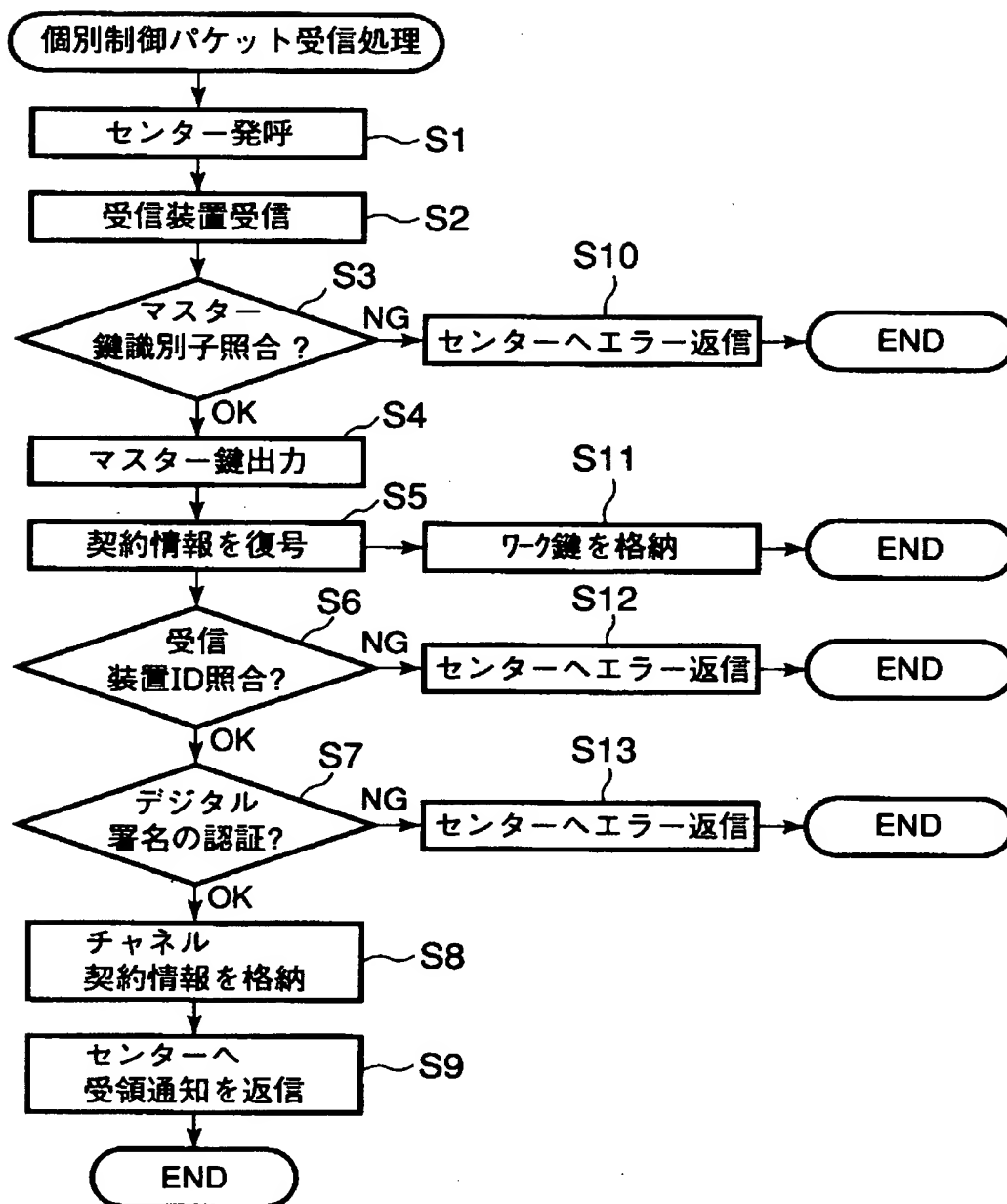
【図 7】



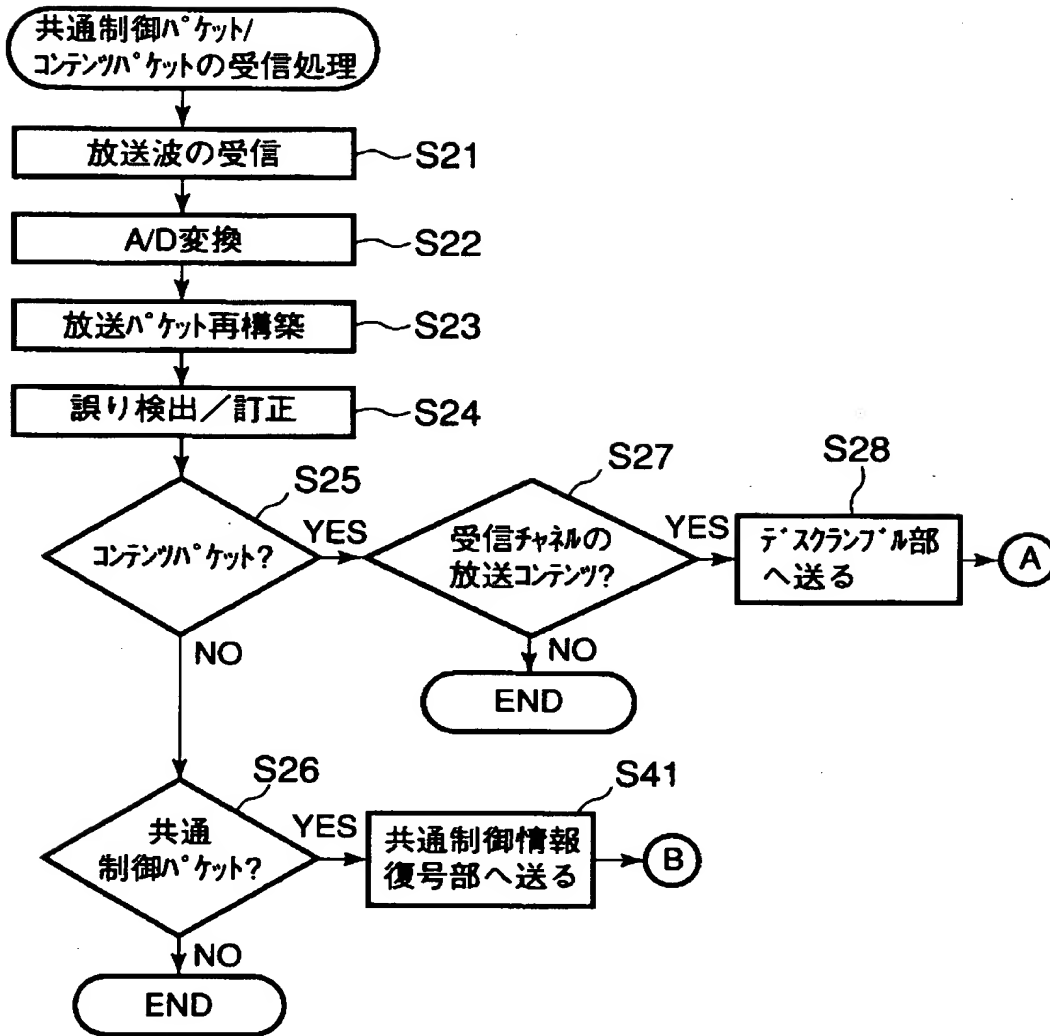
【図 8】



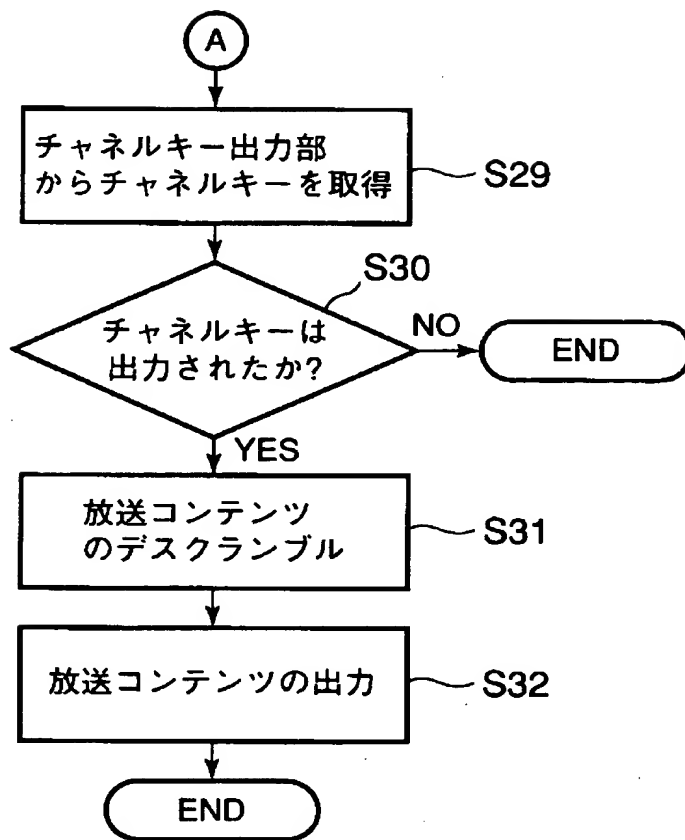
【図 9】



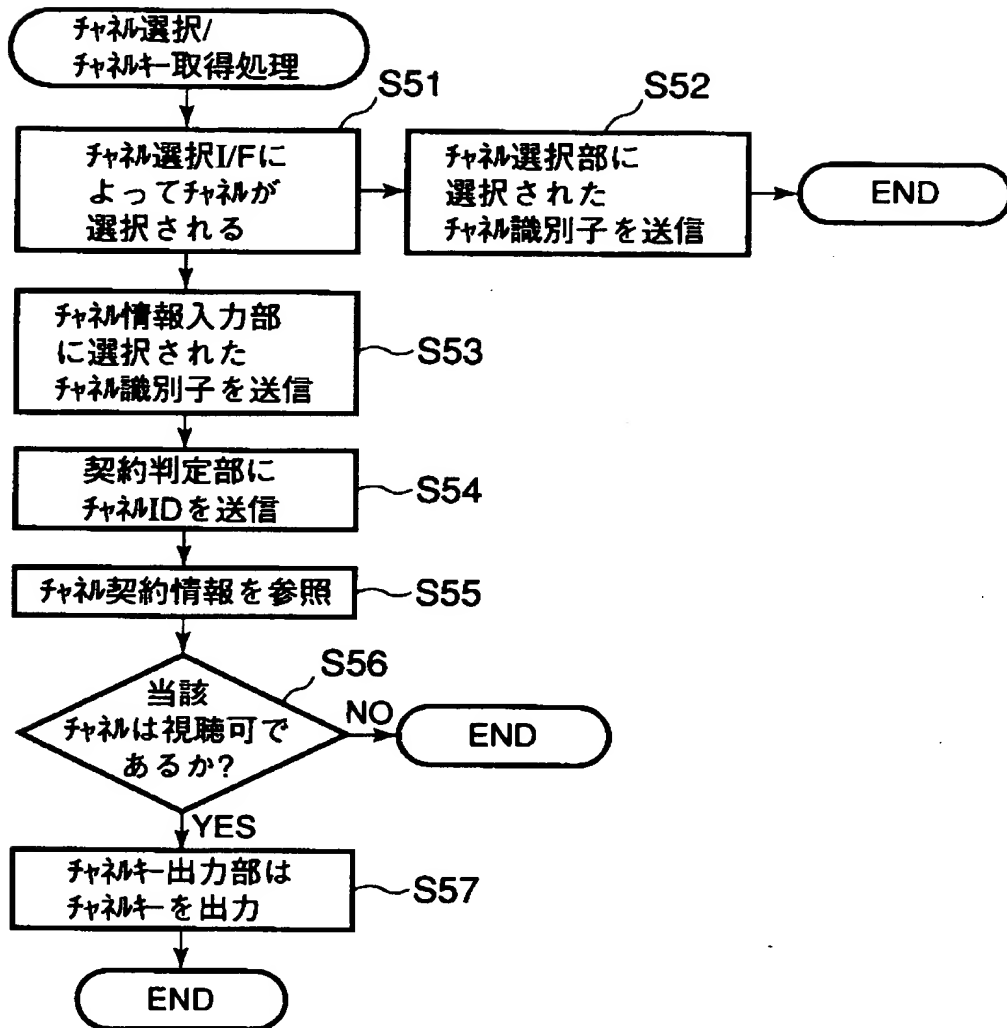
【図 1 0】



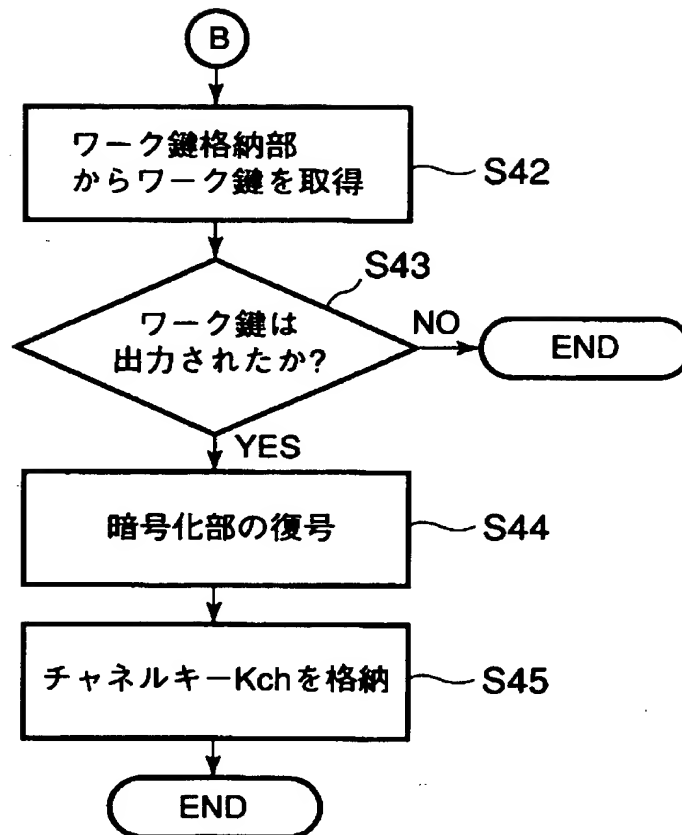
【図 11】



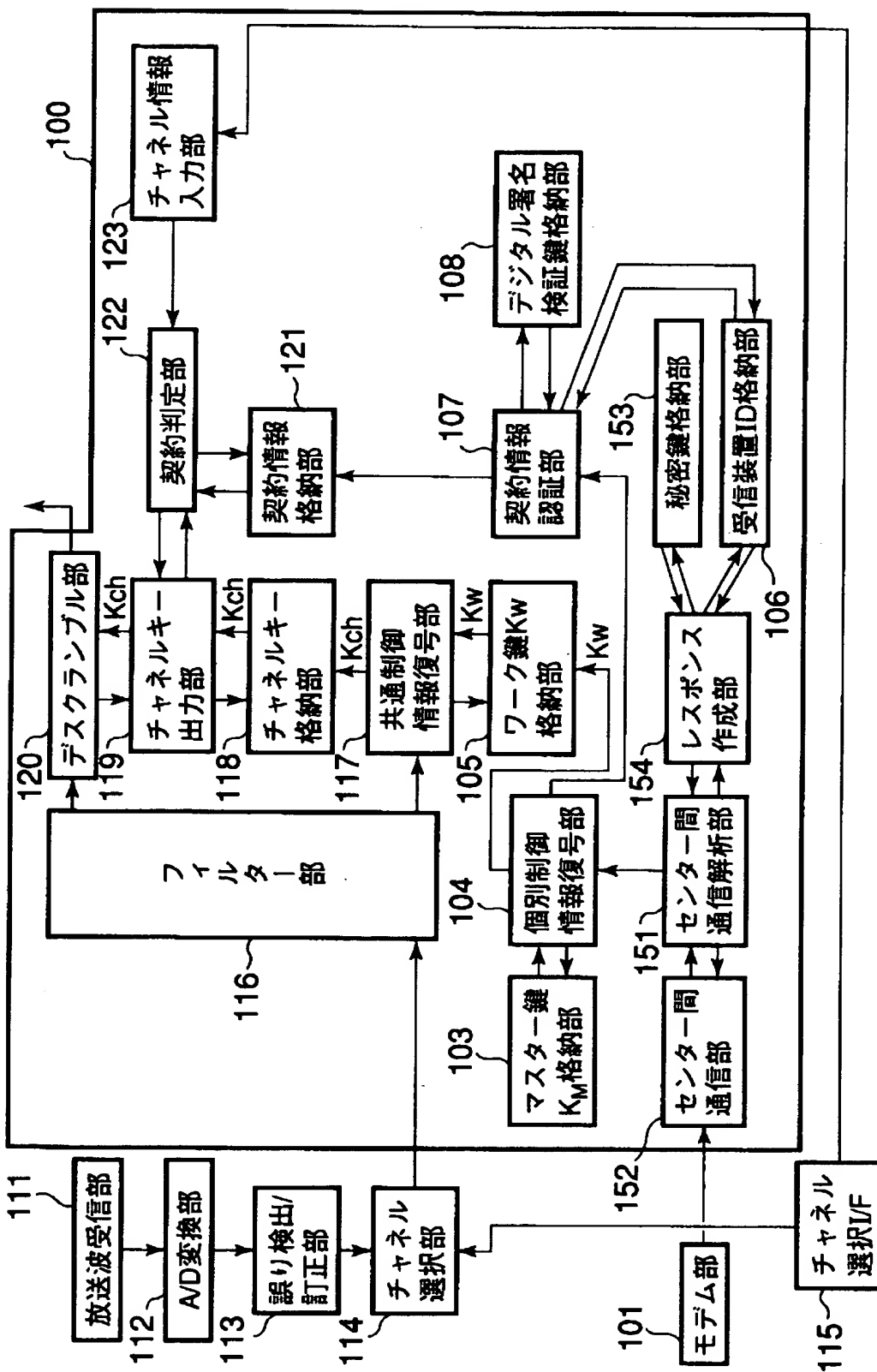
【図 1 2】



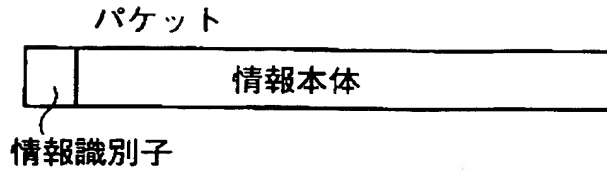
【図 1 3】



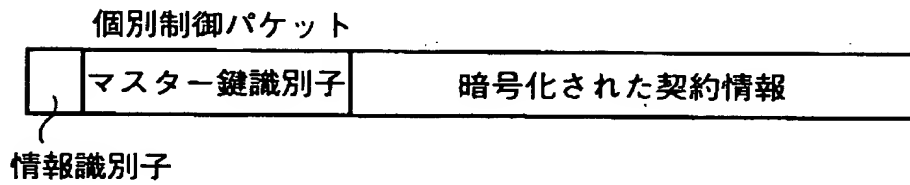
【図 14】



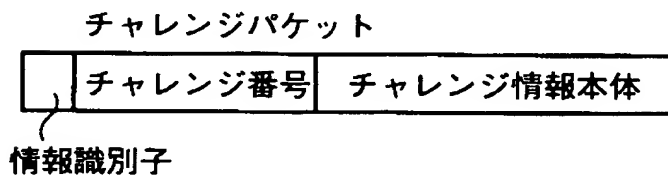
【図 15】



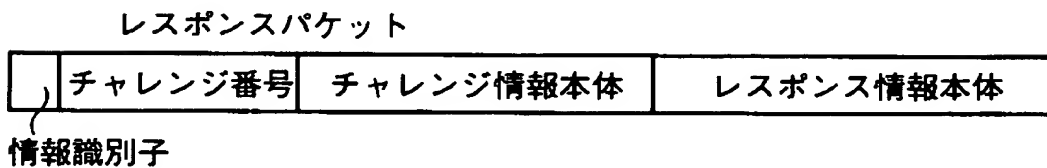
【図 16】



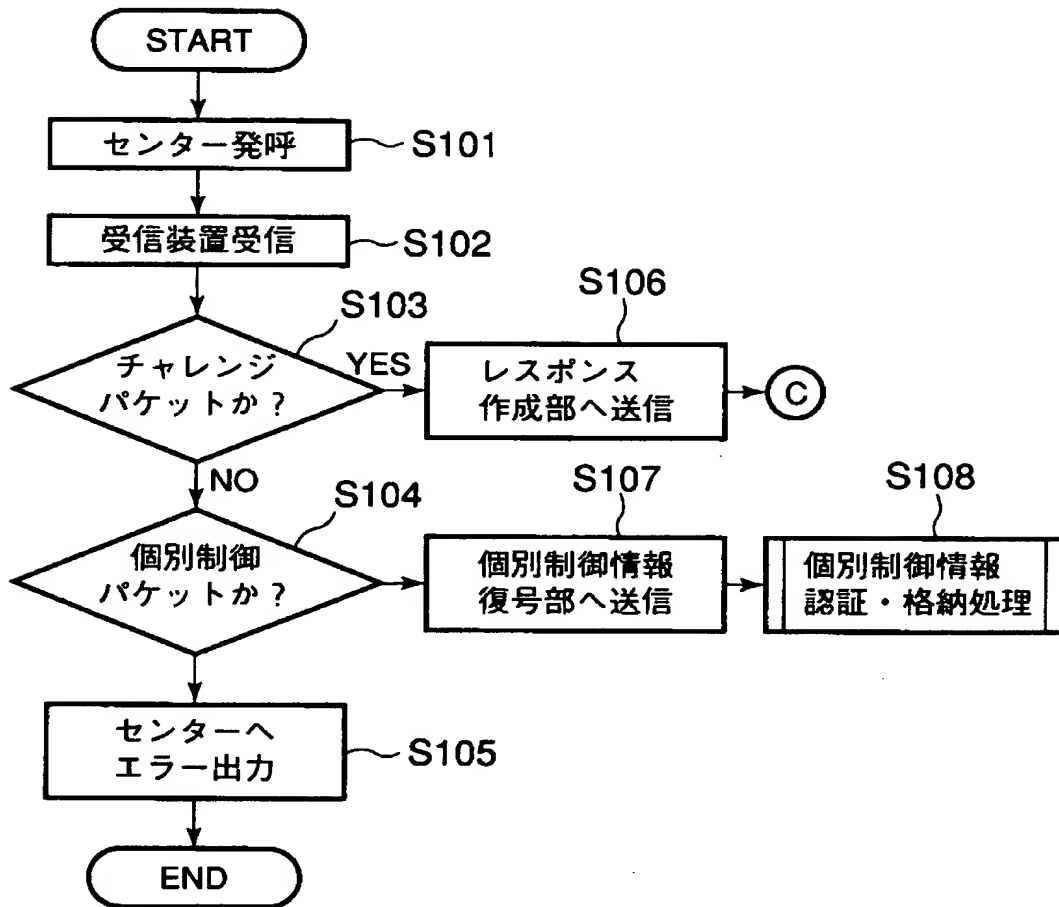
【図 17】



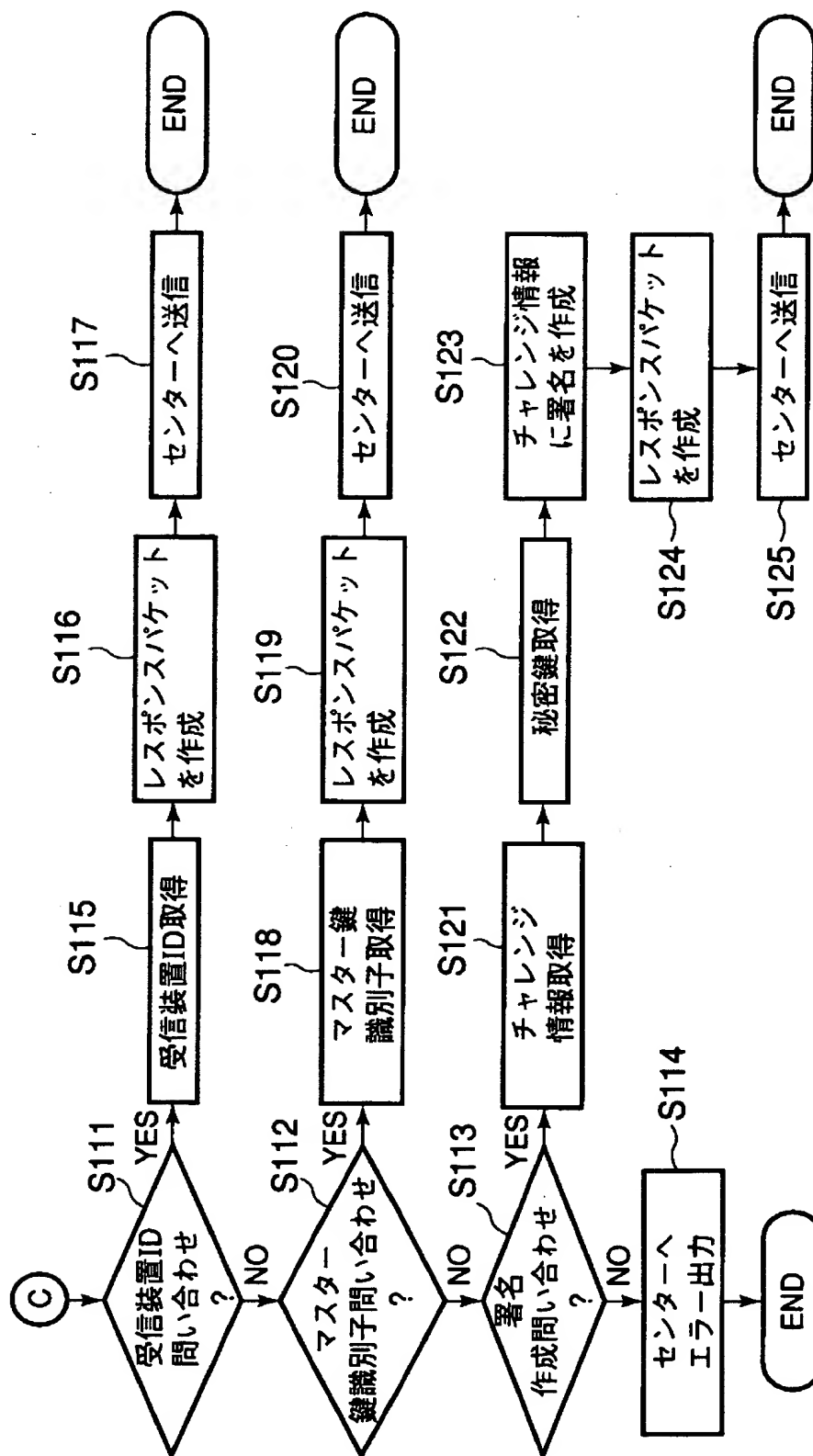
【図 18】



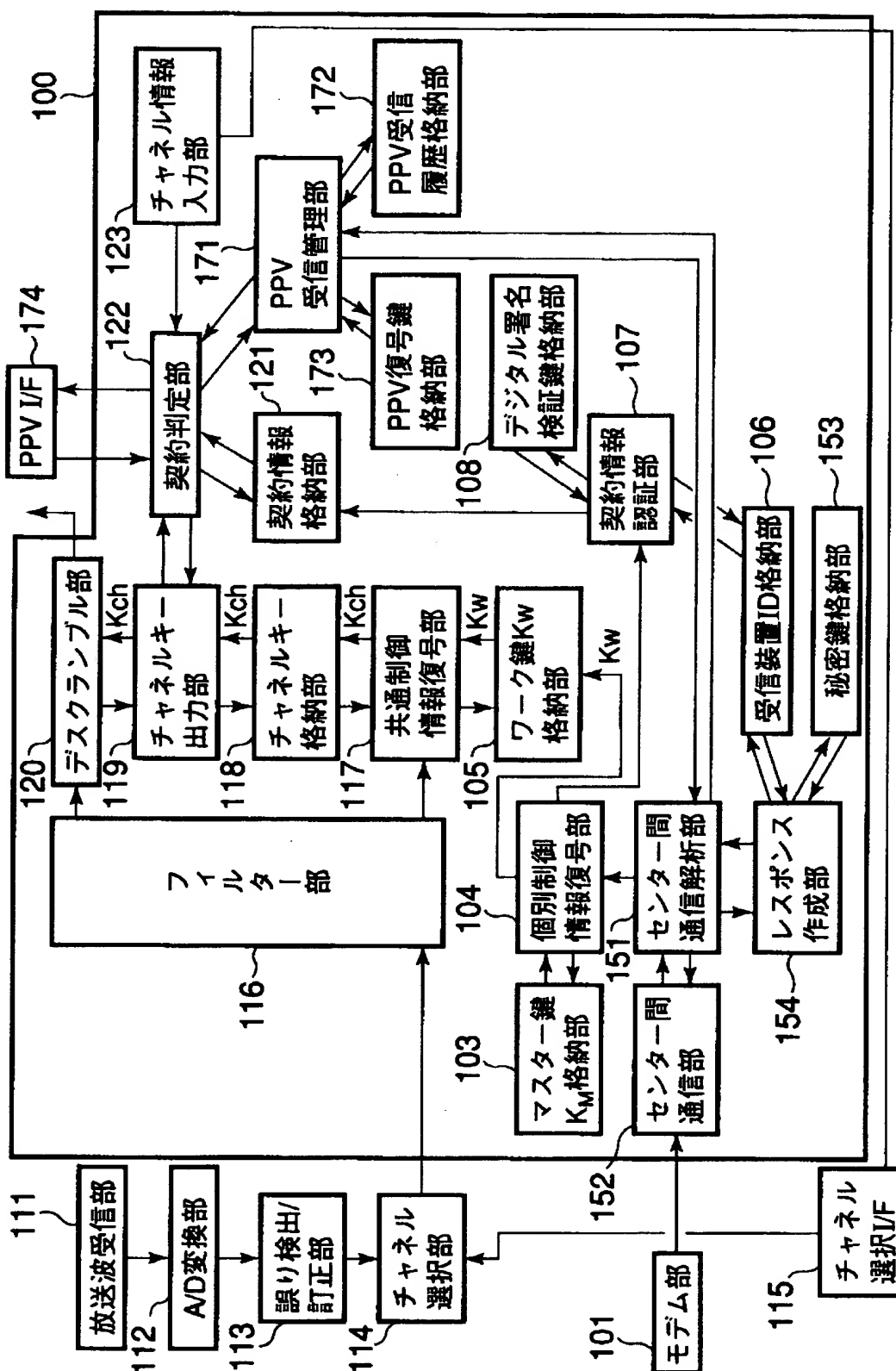
【図 1 9】



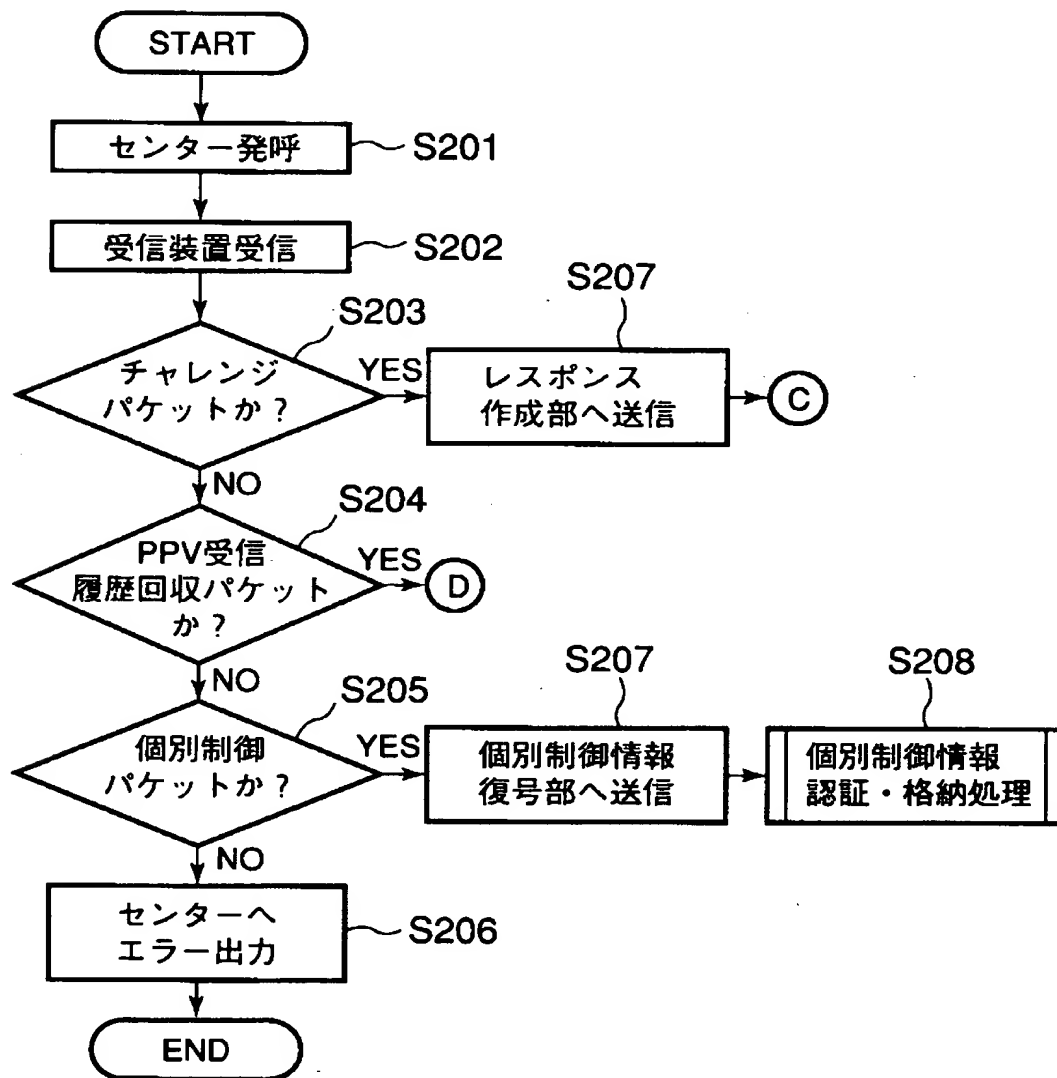
【図 20】



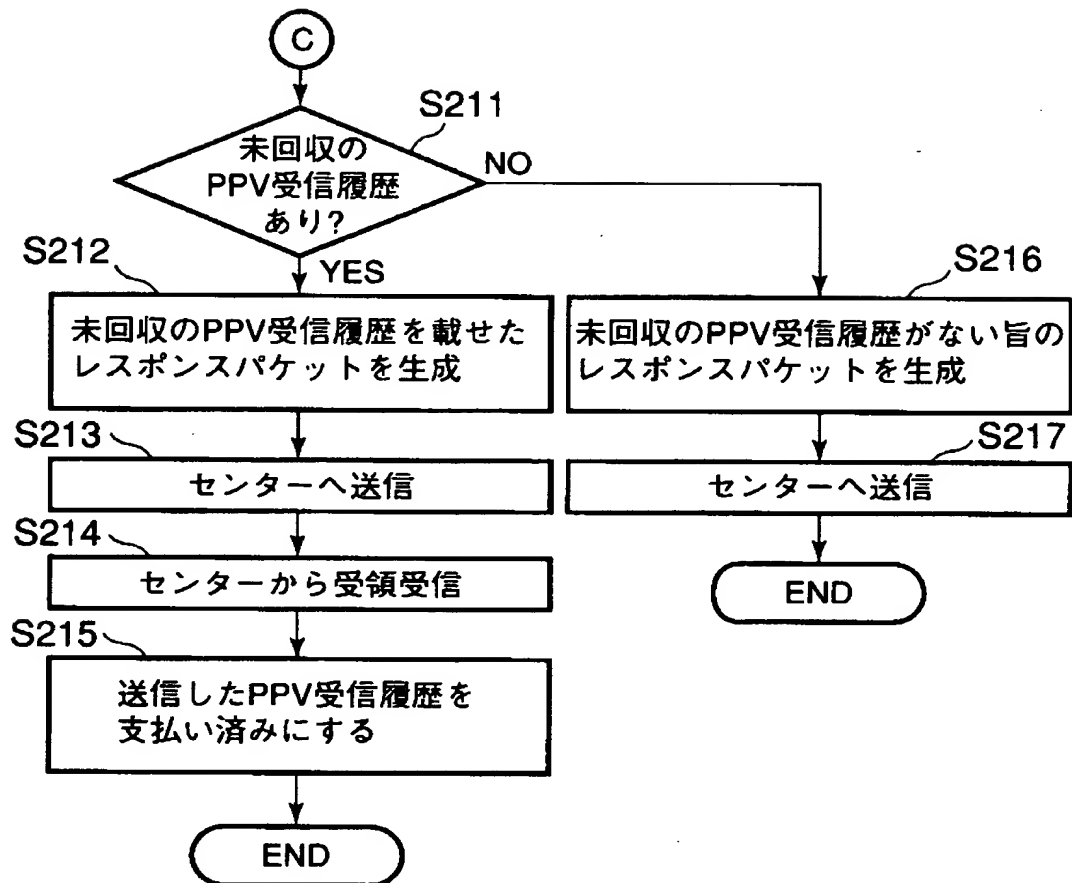
【図 2 1】



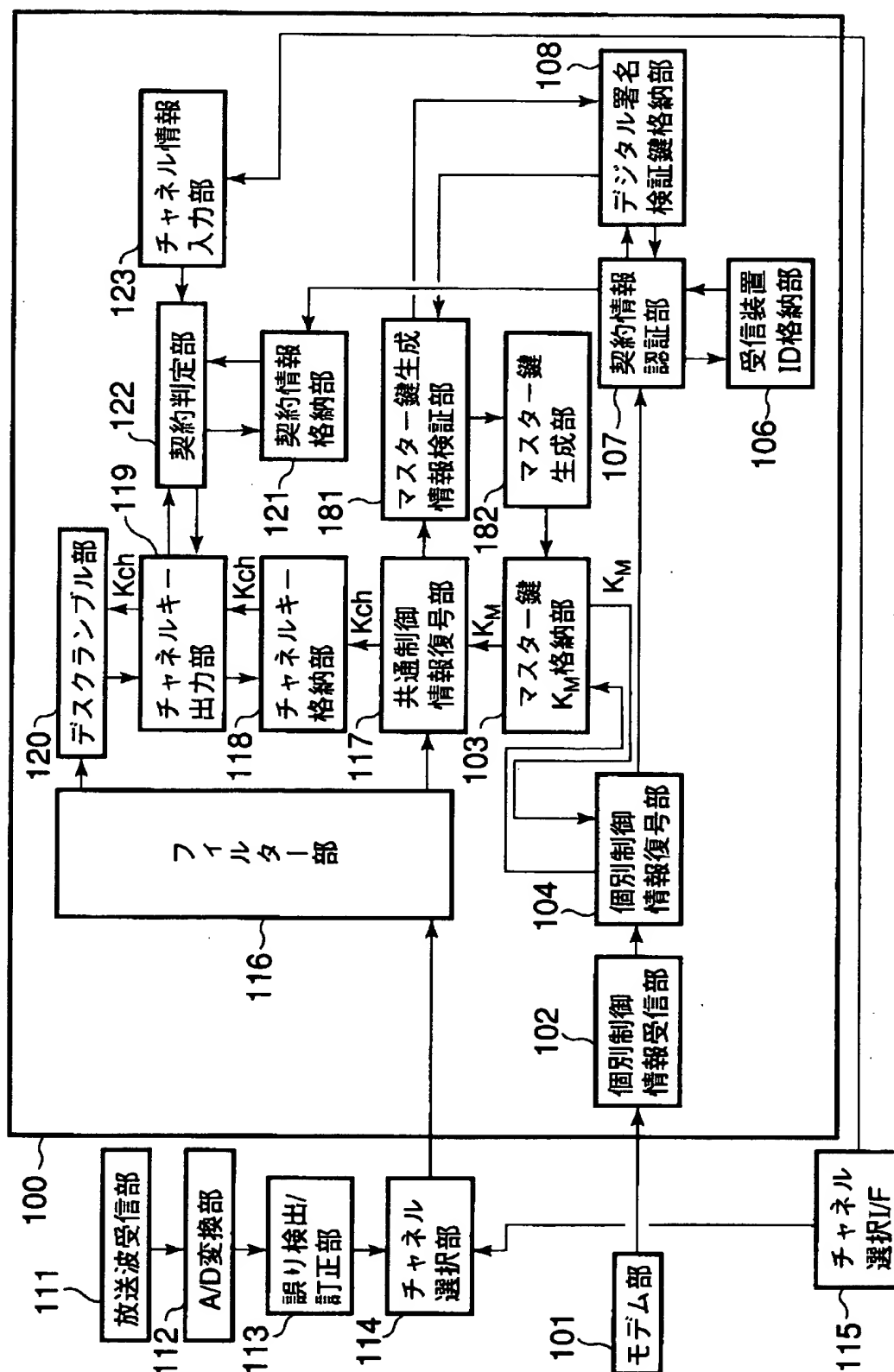
【図 2 2】



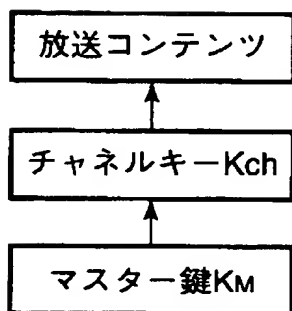
【図 2 3】



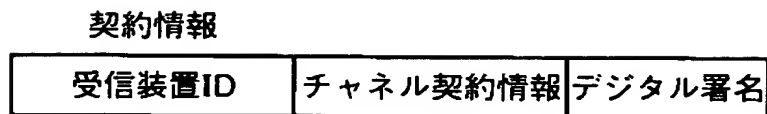
【図 24】



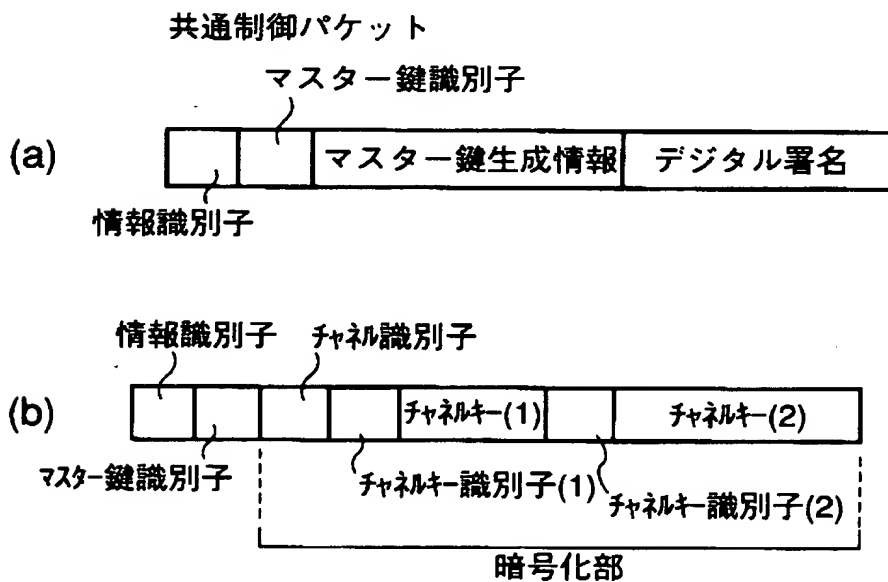
【図 2 5】



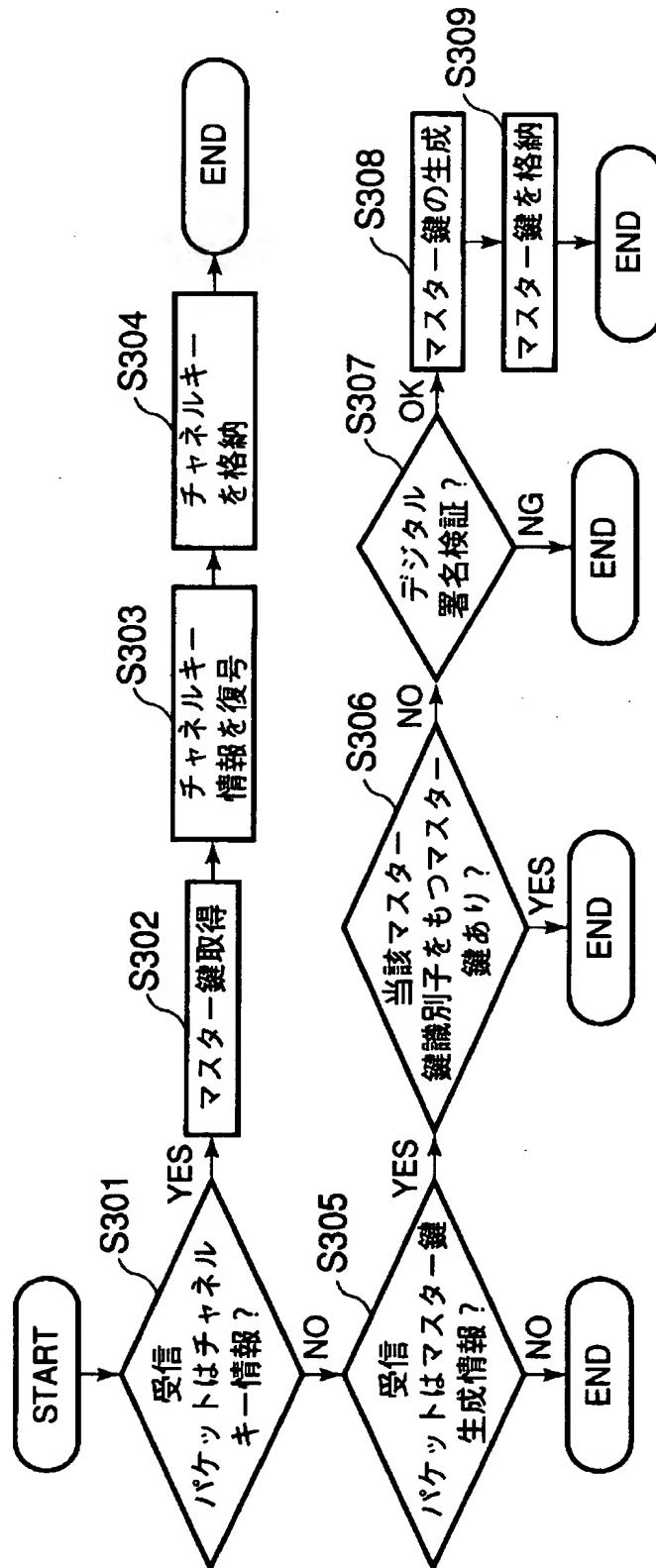
【図 2 6】



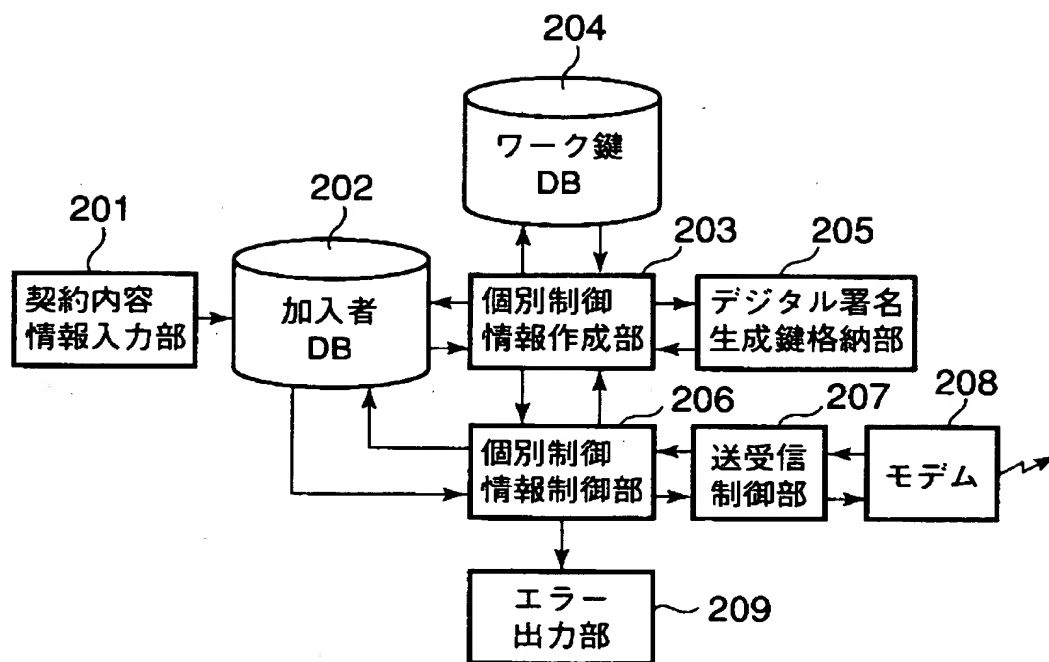
【図 2 7】



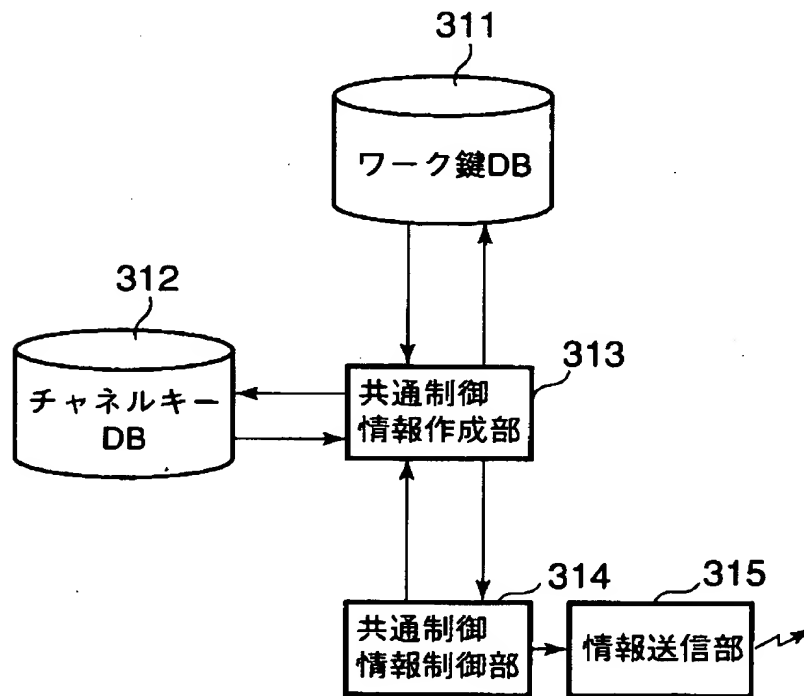
【図 28】



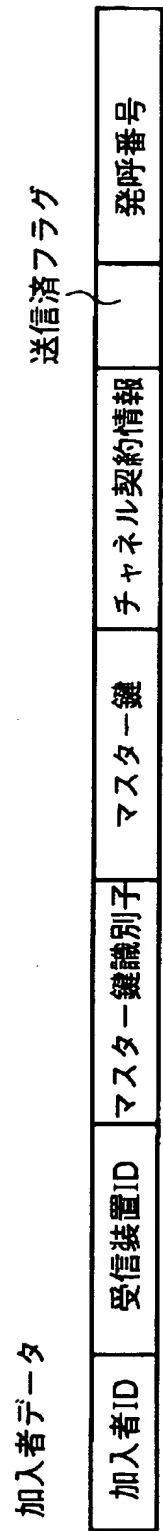
【図 29】



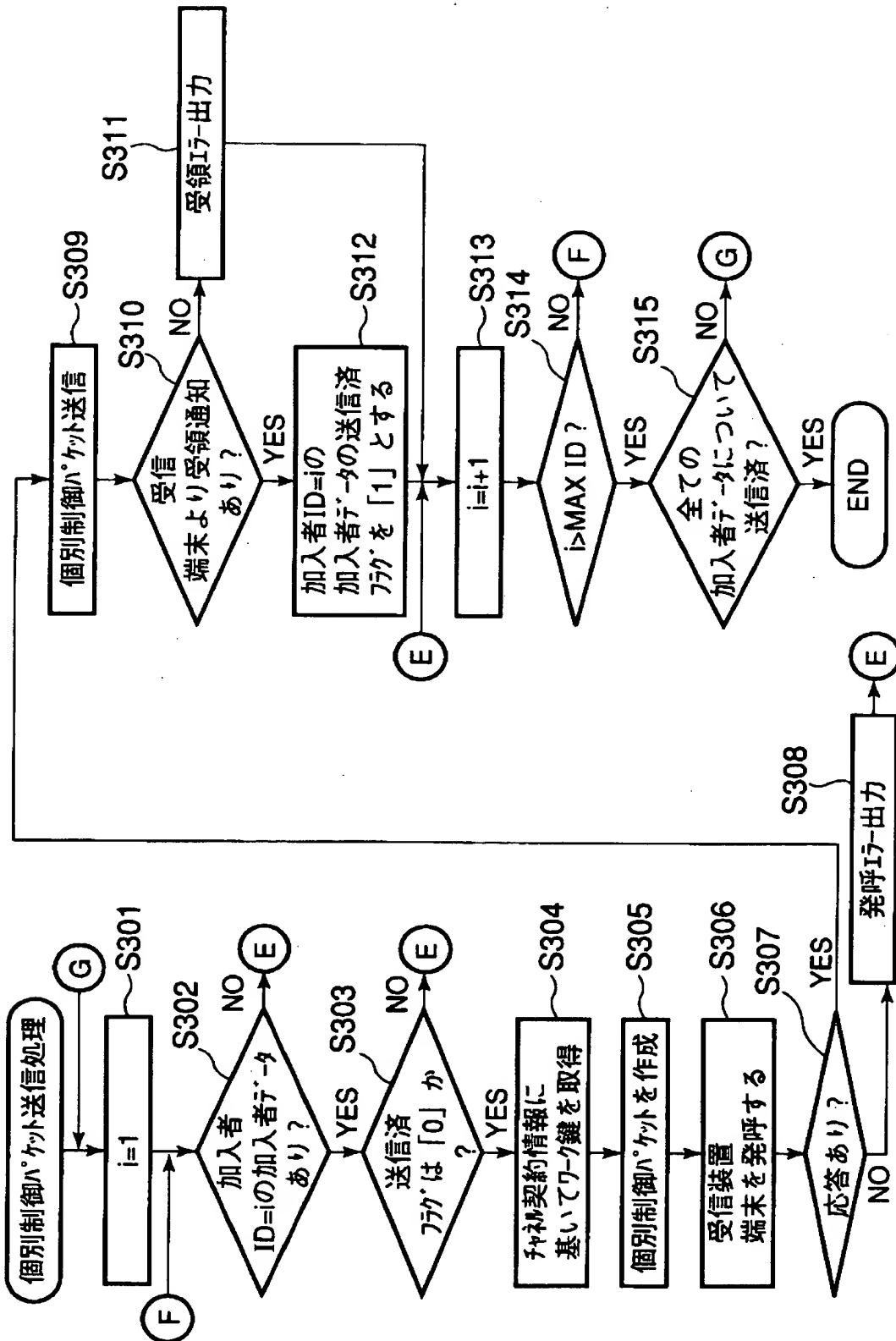
【図 30】



【図 3 1】

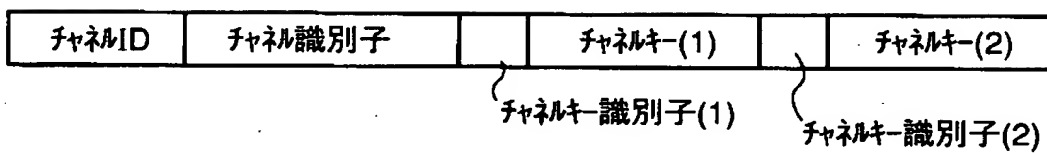


【図 32】

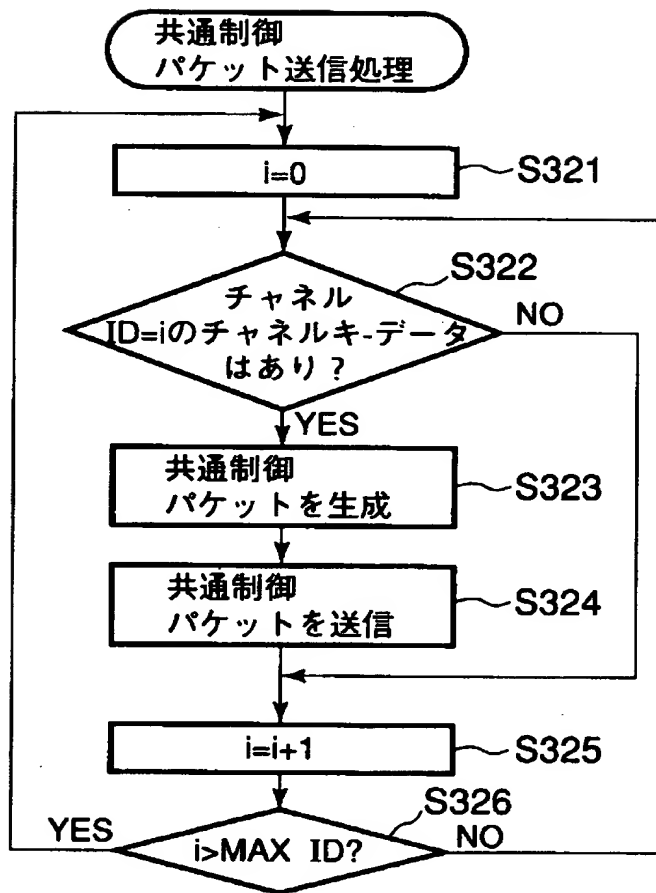


【図 3 3】

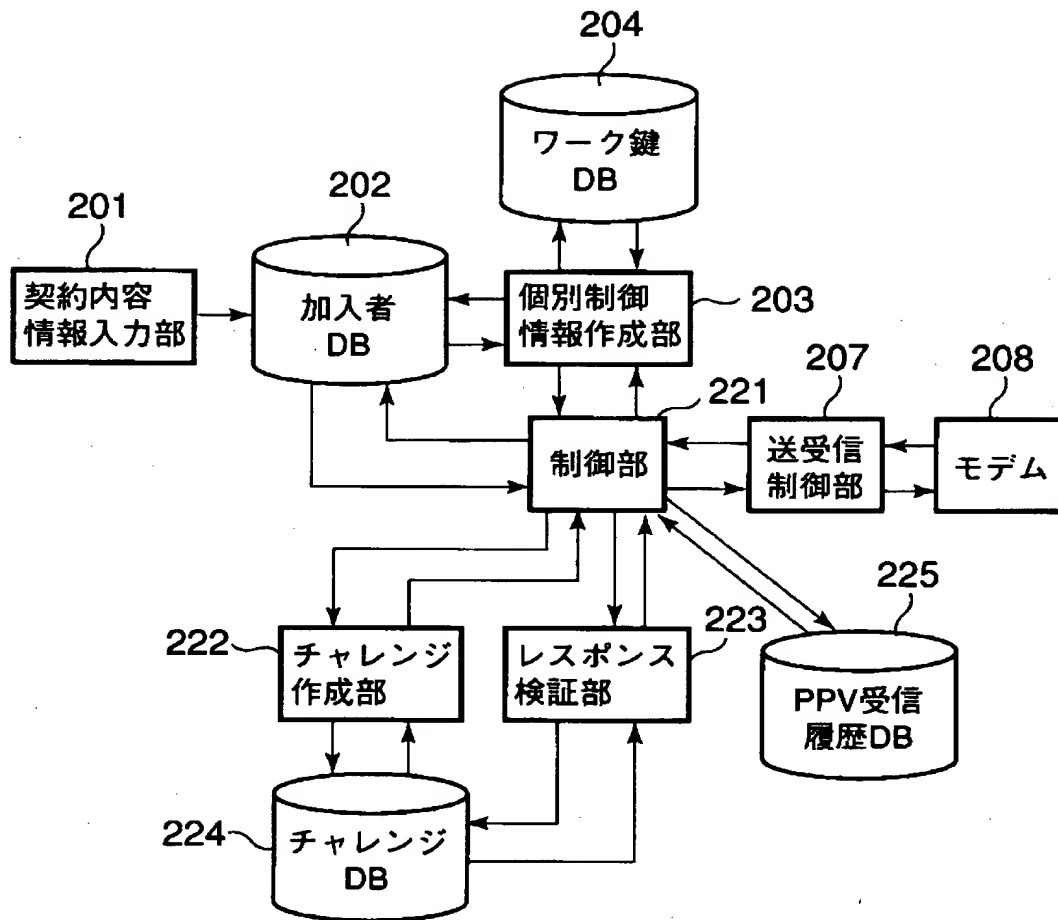
チャンネルキーデータ



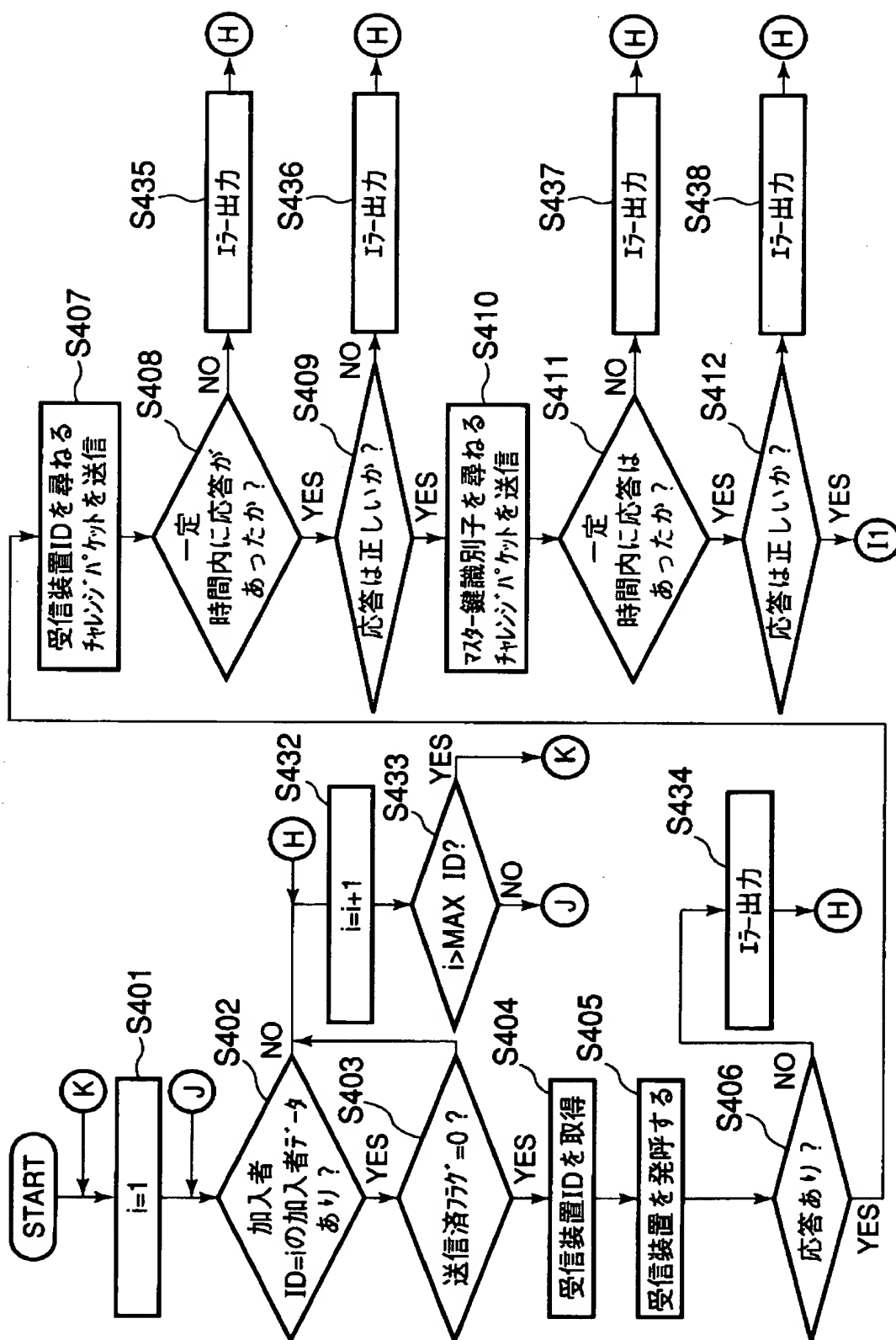
【図 34】



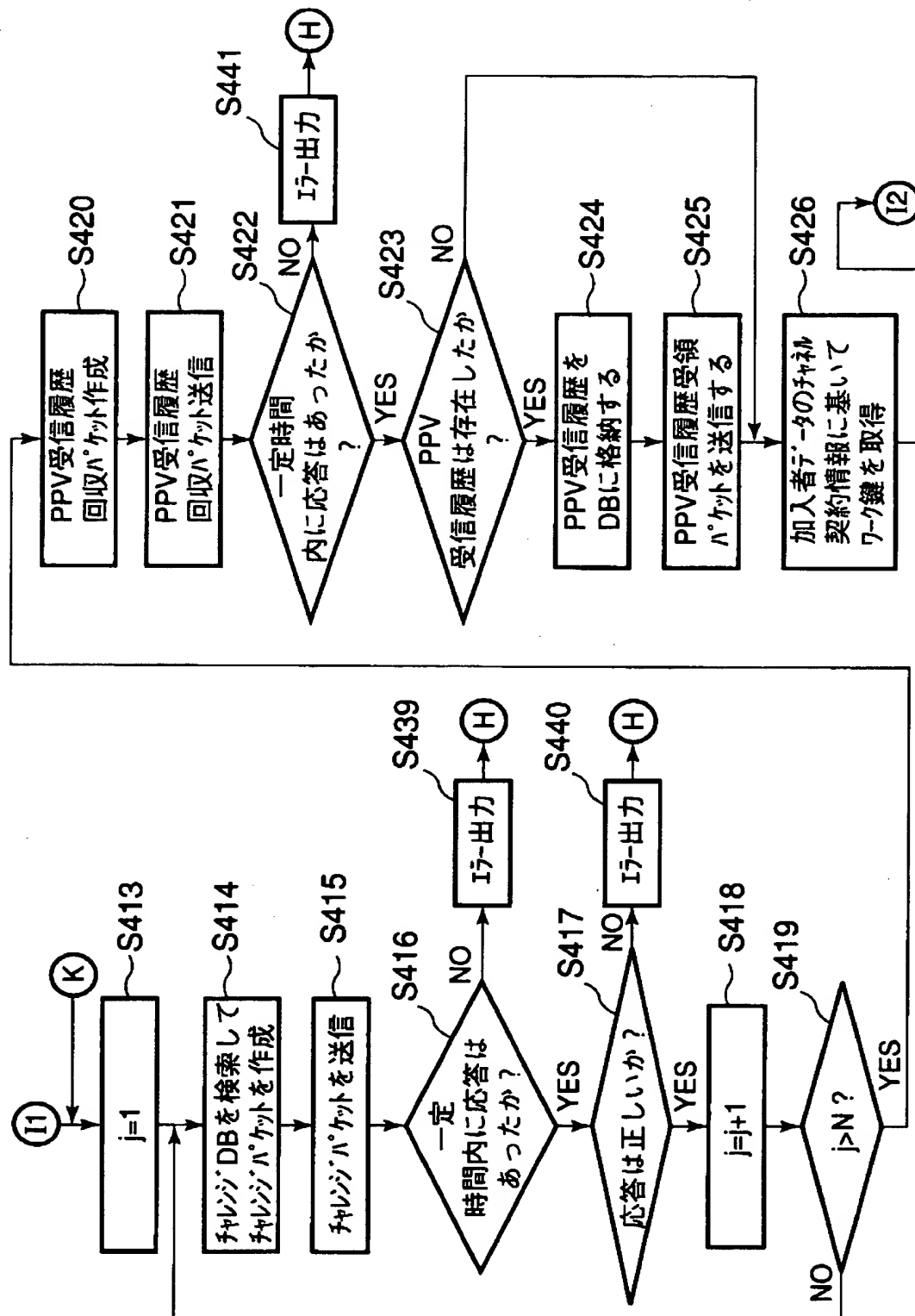
【図 35】



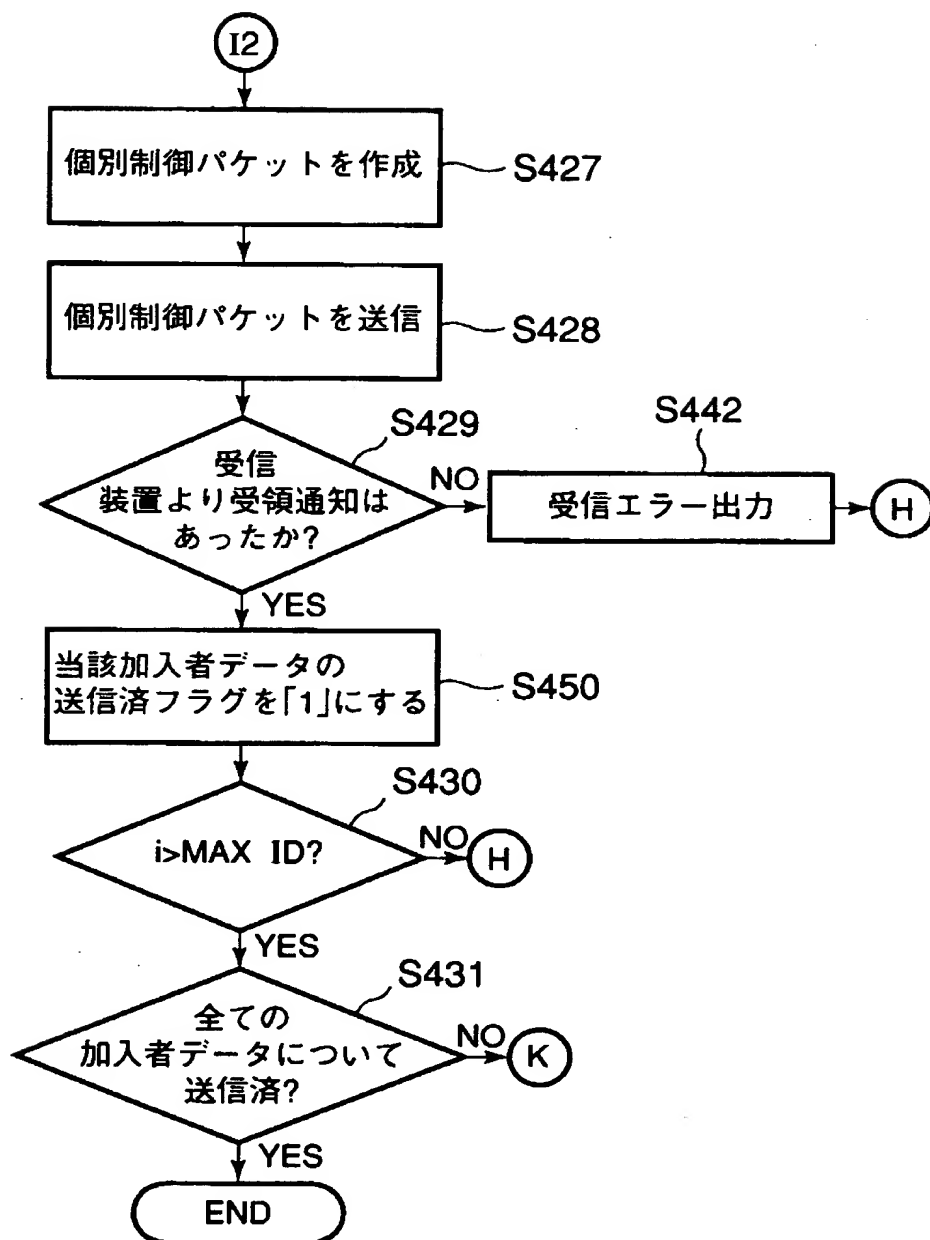
【图 3 6】



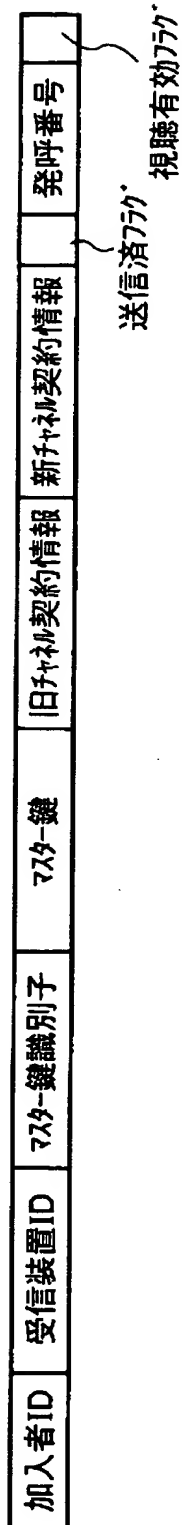
【図 37】



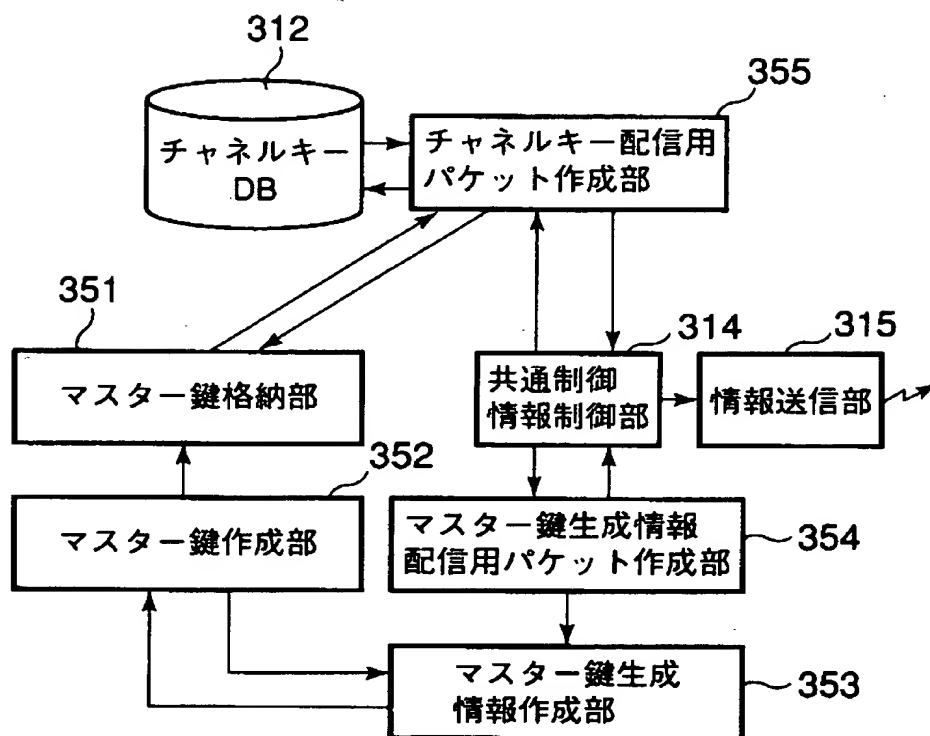
【図 3 8】



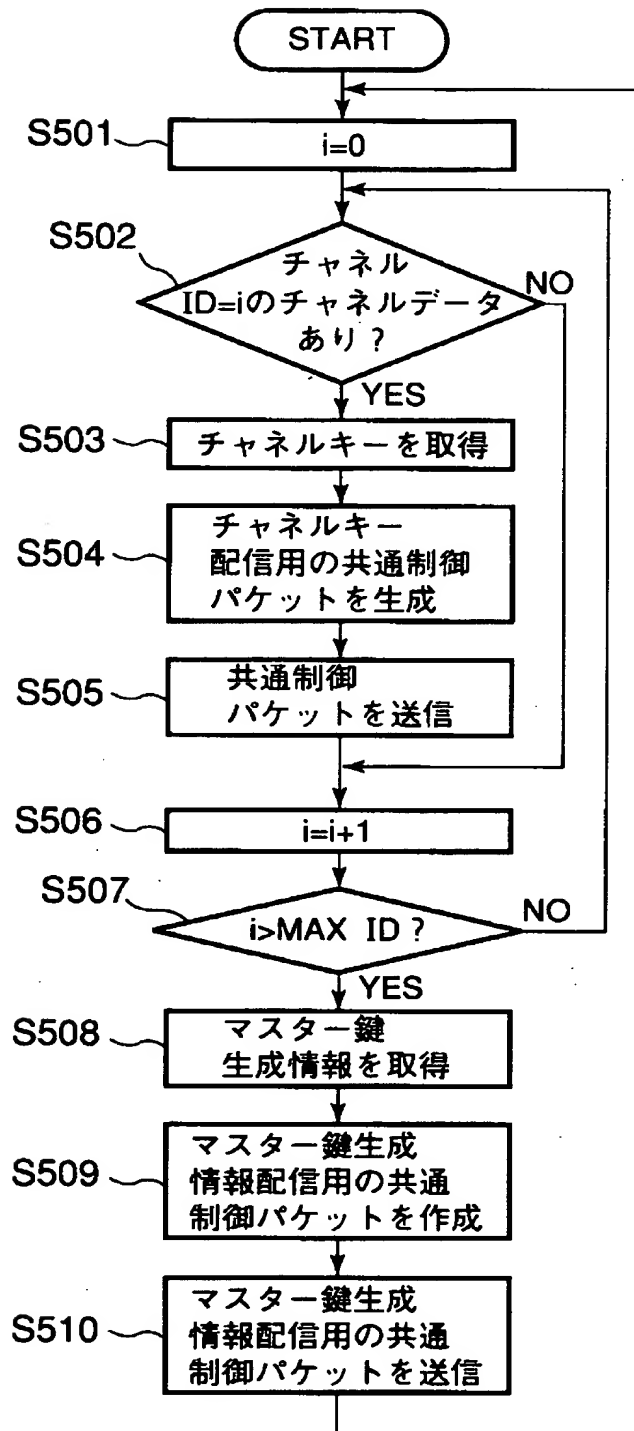
【図 3 9】



【図 4 0】



【図 4 1】



【書類名】 要約書

【要約】

【課題】 加入者が増加しても大量の個別制御情報を配信することにより放送帯域を圧迫することなく、さらに不正な視聴を防止できる安全性の高い有料放送サービスの提供を可能にする。

【解決手段】 放送配信された暗号化されたコンテンツ情報を受信する複数の受信装置のそれぞれが、前記コンテンツ情報の復号を行うために必要な各受信装置に固有の情報を含む復号制御情報を用いて、復号すべきコンテンツ情報を復号するものであって、前記受信装置は、記憶した復号制御情報の一部または全部を更新するための受信装置毎の個別制御情報を双方向通信により受信して前記記憶された復号制御情報を更新するとともに、放送配信された受信装置に依存しないコンテンツ情報を復号するために必要な鍵情報を受信し、この鍵情報と前記復号制御情報とを基に放送配信されたコンテンツ情報を復号する。

【選択図】 図 1

特2000-199629

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝